Centre Africain d'Etudes Supérieures en Gestion

CESAG EXECUTIF

MBA
Audit et Contrôle de Gestion
(MBA-ACG)

Promotion
(2017-2018)

Mémoire de fin d'Etudes

THEME

AUDIT DE LA GOUVERNANCE DU SYSTEME D'INFORMATION DE LA SOCIETE IVOIRIENNE DE RAFFINAGE (SIR)

Présenté par :

M. KONE Nakatanlan Emmanuel

Dirigé par :

Mme Rouba KANE,
Enseignante permanente
Responsable de programmes
MBA ACG, GP et DESCOGEF
CESAG EXECUTIF

Juin 2019

Dédicace

Je dédie ce travail au directeur général de la SIR

M. ***CAMARA Pogabaha Thomas*** *et son conseillé*

M. ***Kader Abdramane OUATTARA****, qui ont financé*

Ma formation dans ce prestigieux établissement.

Remerciements

« Lorsque vous résolvez un problème, vous devriez remercier Dieu et passer au problème suivant. » Dean Rusk.

En préambule à ce travail nous remercions notre Dieu, qui nous aide et nous donne la patience et le courage durant ces longues années d'études.

Aussi, serait-il insoutenable pour nous de poursuivre cette danse de vocables, sans toutefois remercier sincèrement les personnes dont les noms suivent, pour la disponibilité, l'aide et le temps qu'ils voulurent bien manifester à notre égard, et sans qui, ce mémoire n'aurait pu sortir des fonds baptismaux.

Mes premiers remerciements sont adressés à mes parents ***M. KONE Napegadie et Mme KONE Milama Rose Epse KONE*** *pour leur soutien moral et financier, au directeur général de la SIR* ***M. CAMARA Pogabaha Thomas****, M.* ***Kader Abdramane OUATTARA*** *et le directeur général d'atlantique telecom (Moov-CI)* ***M. OUSSALAH Lhoussaine*** *pour leur soutien financier.*

Ensuite je remercie mes enseignants et enseignantes du ***CESAG*** *pour leur contribution à notre formation du MBA en audit et contrôle de gestion et je remercie particulièrement mon encadreur pédagogique* ***Mme Rouba KANE****.*

Enfin, bien sûr, je tiens à remercier le responsable de la structure informatique ***M. ADON****, le responsable infrastructure* ***M. Antonio*** *pour leur encadrement et la responsable de la structure politique école* ***Mme COULIBALY Korotum*** *pour son coaching, leurs recommandations précieuses et leur disponibilité, ainsi que* ***M. EDOH Hugues*** *maitre de stage qui m'a guidé lors du stage.*

Listes des figures

Liste des tableaux

Liste des annexes

Liste des Sigles et abréviations

Sigles et abréviations	désignation
AFAI	**A**ssociation **F**rançaise de l'**A**udit et du **C**onseil **I**nformatiques
Cobit	**C**ontrol **O**bjectives for **I**nformation and related **T**echnology
FRAP	**F**euille de **R**évélation et d'**A**nalyse De **P**roblème
IEC	**I**nternational **E**lectronical **C**ommission
IFACI	**I**nstitut **F**rançais de l'**A**udit et du **C**ontrôle **I**nterne
IIA	**I**nstitute of **I**nternal **A**uditors
IP	**I**nternet **P**rotocol
ISACA	**I**nformation **S**ystems **A**udit and **C**ontrol **A**ssociation
ISO	**I**nternational **O**rganization for **S**tandardization
LAN	**L**ocal **A**rea **N**etwork (Réseau Local)
OS	**O**perating **S**ystem
RSSI	**r**esponsable **s**écurité des **S**ervices **I**nformatiques
SI	**S**ystèmes d'**I**nformation
SIR	**S**ociété **I**voirienne de **R**affinage

SOMMAIRE

INTRODUCTION GENERALE

Contexte

La gouvernance des SI est un domaine de la gouvernance de l'organisation basée sur la technologie et l'information. Elle comprend la direction, les structures organisationnelles et les processus qui garantissent que les systèmes d'information soutiennent la stratégie et les objectifs de l'organisation. La gouvernance des SI soutient les exigences réglementaires, légales, environnementales et opérationnelles de l'organisation pour lui permettre d'atteindre ses plans et ses ambitions stratégiques.

Bien que la technologie offre des opportunités de croissance et de développement, elle s'accompagne également de menaces telles que des dysfonctionnements, des manœuvres répréhensibles, des vols et des fraudes. Les recherches montrent que les organisations sont menacées par des attaques externes, néanmoins les personnes de confiance, bien informées, représentent une menace bien plus importante. Heureusement, la technologie peut également protéger des menaces, par des missions d'audit afin de mieux évaluer les risques et se protéger. C'est ainsi, le référentiel COBIT, Control objectives for information and technology, qui conçu par l'ISACA (Information Systems Audit and Control Association) il y a déjà une bonne dizaine d'années, est un cadre de référence et un ensemble d'outils jugés indispensables pour assurer la maîtrise et surtout le suivi (audit) de la gouvernance du SI dans la durée. COBIT est fondé sur un ensemble de bonnes pratiques collectées auprès d'experts SI de divers secteurs (industrie et services).

Problématique

La Société Ivoirienne de Raffinage qui suit les différentes mutations à l'instar de toutes les sociétés modernes est dotée d'un système d'information qui souffre d'une gouvernance assez mitigée.

En effet, j'ai été affecté premièrement, à la structure budget reporting, ensuite à la structure informatique, enfin à la structure gouvernance et contrôle interne de la SIR, mais sous la couverture de la structure audit interne. Nous avons pris connaissance de manière transversale des problèmes liés à la gouvernance des systèmes d'information de la SIR.

A sa création la SIR n'avait pas défini de structure de gouvernance formelle, elle se contentait à produire et vendre ses produits pétroliers. C'est après la crise financière qu'elle a vécu entre 2008 et 2013 qu'elle a enfin créée une structure de gouvernance, qui à ce jour n'a pas encore prévu l'alignement de son système d'information à la stratégie de l'entreprise. Il faut noter que l'architecture de son système d'information avait été conçue de manière statique.

En plus, Créée avec 100 personnes elle a opté auprès de son fournisseur réseau des adresses uniquement publiques. Chacun de ses agents était sur le même segment réseau ce qui sous-entend que tout agent peut bénéficier même d'informations confidentielles ne le concernant pas. Les différents bureaux assez larges n'ont qu'une seule prise réseau pour trois ou quatre postes. Ce qui fait qu'on est obligé d'avoir dans chaque bureau un seul câble Ethernet branché à la prise et à un switch. A ce switch sont connectés les postes des différents utilisateurs, les imprimantes et scanners.

De plus la structure informatique n'a pas une bonne communication avec les différents services métiers. Ce fait est visible avec la migration de sage vers SAP. En effet, certains disent préférer sage qui leur permettaient par exemple d'avoir l'écart (réel) de trésorerie en fin de journée et le solde prévisionnel de leur trésorerie sur trois jours. Ce qui ne leur ait plus possible du fait de la non-maitrise du nouveau logiciel.

Aujourd'hui avec la saturation de son réseau et l'attaque du ransomware (phobos) [1] qu'elle a subie, la SIR commence à prendre conscience de la notion de gouvernance des systèmes d'information.

Question centrale

Quelle amélioration faut-il de la gouvernance du système d'information de la SIR, pour faire face aux risques qui ont facilité son attaque et qui mettent en mal la productivité de la SIR ?

Questions spécifiques

Pour mieux répondre à la question centrale nous l'avons décomposé en questions spécifiques :

- La structure informatique se présente t'elle selon la structuration de la norme Cobit 5 ?
- La structure informatique communique t'elle sur le risque de sécurité lié au système d'information ?
- La SIR a-t-elle une politique de sécurité bien élaborée dont les agents ont connaissance ?
- Quelle amélioration pour la gouvernance du système d'information de la SIR ?

[1] Phobos Ransomware est un cheval de Troie crypté qui a été observé pour la première fois le 21 octobre 2017. Le logiciel Phobos Ransomware est utilisé pour cibler les utilisateurs d'ordinateurs d'Europe occidentale des États-Unis et transmet ses messages de rançon en anglais aux victimes. La SIR a été victime de ce virus le 25 février ce qui nous a motiver à faire l'audit de la gouvernance de la SIR.

Objectif général

L'objectif général de ce travail est de mettre à nu les risque liés à la gouvernance du système d'information de la SIR et faire des recommandations afin d'améliorer sa productivité[2].

Objectifs spécifiques

Les objectifs spécifiques du travail sont :

- ✦ Diagnostiquer la structuration du système d'information de la SIR comparativement à la norme Cobit 5 ;
- ✦ Identifier les risques liés à la gouvernance des SI de la SIR ;
- ✦ Apprécier la politique de sécurité du système d'information de la SIR ;
- ✦ Proposer une architecture de la structure informatique et rédiger une charte informatique pour la SIR.

Intérêt du thème

L'intérêt que regorge notre étude peut être situé à deux niveaux :

- **Pour l'entreprise :** elle pourra disposer des meilleures pratiques en termes de maintenance et amélioration continue du système de sécurité de l'information, dynamiser ses fonctions et être plus attractive de par ses services métiers. Aussi elle saura ce dont elle a besoin en matière d'outils, de techniques, et de moyens tant humains que matériels pour assurer la gouvernance de son système d'information.
- **Pour nous même :** cette étude sera une occasion pour nous de confronter nos connaissances théoriques à celles pratiques acquises pendant nos moments de formation professionnelles. Il s'agira pour nous d'avoir une connaissance plus élaborée sur la gouvernance des systèmes d'information et la contribution de l'audit interne à résoudre les problèmes liés à cette gouvernance.
- **Pour la communauté scientifique :** L'intérêt scientifique de ce travail repose sur le fait qu'il se veut une contribution à la problématique portant sur la gouvernance du système d'information des entreprises. La menace cyber sécurité est aujourd'hui réelle et aucune entreprise, étatique ou non étatique n'est à l'abri de cette nébuleuse. La présente étude entend se focaliser davantage sur la bonne connaissance des risques que connait la gouvernance des systèmes d'information. Dans ce contexte, elle se pose avec

[2] L'attaque Phobos a entrainé la SIR dans une période d'inactivité d'un mois. Donc les managers de chaque structure ont dû mettre en place un budget pour le paiement d'heures supplémentaires des agents techniques.

acuité du fait que la SIR est affectée par des vulnérabilités structurelles et techniques qui la fragilise.

Annonce du plan

Pour atteindre les objectifs que nous nous sommes fixés, notre travail sera décomposé en deux parties.

Une première partie, qui aborde la revue de la littérature sur l'audit de la gouvernance des systèmes d'information et la méthodologie de recherche. Elle sera composée de deux chapitres dont le premier chapitre est basé sur la revue de la littérature sur l'audit de la gouvernance des systèmes d'information. Et le deuxième chapitre sur la méthodologie de recherche.

Une deuxième partie pratique qui aborde le cadre pratique de l'audit de la gouvernance du système d'information de la SIR, et qui est repartie en deux chapitres. Le troisième Chapitre concerne la présentation de la SIR, et le quatrième s'occupe de la réalisation de l'audit de la gouvernance du système d'information de la SIR et des recommandations qui en découlent.

PREMIERE PARTIE : REVUE DE LA LITERATTURE SUR L'AUDIT DE LA GOUVERNANCE DES SYSTEMES D'INFORMATION ET METHODOLOGIE DE RECHERCHE.

La gouvernance des systèmes d'information est un domaine très vaste puisqu'elle fait appel à toutes les entités de l'entreprise et à des connaissances techniques et technologiques de pointe. L'une des forces et en même temps une problématique du monde des affaires actuel est l'évolution constante des technologies de l'information. Il est vrai que plus les technologies évoluent, plus elles offrent une plus grande mobilité aux utilisateurs et révolutionnent les habitudes et les façons de travailler. Cependant elles sont empreintes de risques de plus en plus forts. Il faudrait donc trouver des solutions de gouvernance de l'information pour mieux adapter le système d'information à l'atteinte des objectifs stratégiques de l'entreprise.

Dans cette quête de solutions et de bonnes pratiques de gouvernance, l'entreprise dispose d'agents régulateurs, garant des dispositifs de contrôle interne tel que l'audit interne. A cet effet, différents auteurs ont développé plusieurs théories et avis mettant en exergue le rôle de l'audit interne dans la gouvernance des systèmes d'information. Nous nous sommes par conséquent attelés à présenter ces différentes opinions dans notre cadre théorique afin d'avoir une meilleure compréhension de l'audit de la gouvernance des systèmes d'information. Cette partie sera aussi l'occasion d'aborder la partie méthodologie de notre étude.

CHAPITRE 1 : revue de la littérature sur l'audit de la gouvernance des SI

Dans ce premier chapitre nous traiterons dans une première partie le cadre théorique, conceptuel de l'audit interne et de la gouvernance des systèmes d'information. Dans une deuxième, nous ferons l'état des connaissances sur l'audit de la gouvernance des systèmes d'information.

1.1. Notion d'audit

Celui-ci est défini par IFACI & al. (2000 : 33), comme une « démarche spécifique d'examen et d'évaluation des activités d'une organisation, fondée sur un référentiel et dont les conclusions peuvent comporter des propositions d'amélioration touchant à la régularité et/ou la performance ».

Becour & al. (2008 : 12) pour leur part, considèrent que l'audit est « une activité qui applique en toute indépendance des procédures cohérentes et des normes d'examen en vue d'évaluer l'adéquation, la pertinence, la sécurité et le fonctionnement de tout ou partie des actions menées dans une organisation par référence à des normes».

Ces deux définitions nous permettent d'affirmer que l'audit est une activité d'assurance et de conseil qui consiste pour un agent (interne ou externe à l'entité) compétent et impartial à donner un jugement, une appréciation sur les activités d'une organisation et sur le fonctionnement.

Il existe deux types d'audit à savoir :

- L'audit externe qui Selon l'IFACI, l'audit interne est une fonction où les auditeurs externes eux, ne sont pas partie prenante dans le dispositif de contrôle interne et de gestion des risques de l'entreprise. Mais ils prennent connaissance de ce système pour en obtenir une meilleure compréhension et La coopération entre auditeurs internes et auditeurs externes est un vrai sujet, toujours actuel, car cette coopération est aujourd'hui admise et reconnue pour le bien de tous, l'entreprise au premier chef. Chez Sodexo, l'audit interne et l'audit externe travaillent en étroite relation, même si les champs de couverture ne sont pas toujours les mêmes. Leur champ d'intervention est naturellement plus orienté sur le troisième et surtout le deuxième objectif du contrôle interne, c'est-à-dire les objectifs liés au reporting et plus particulièrement celui sur la fiabilité des informations comptables et financières.
- L'audit interne que nous développerons ci-dessous.

1.2. Cadre théorique et conceptuel de l'audit interne et de la gouvernance des systèmes d'information.

Cette partie s'intéresse premièrement au cadre théorique et conceptuel de l'audit interne et deuxièmement au cadre théorique et conceptuel de la gouvernance des systèmes d'information.

1.2.1. Cadre théorique et conceptuel de l'audit interne

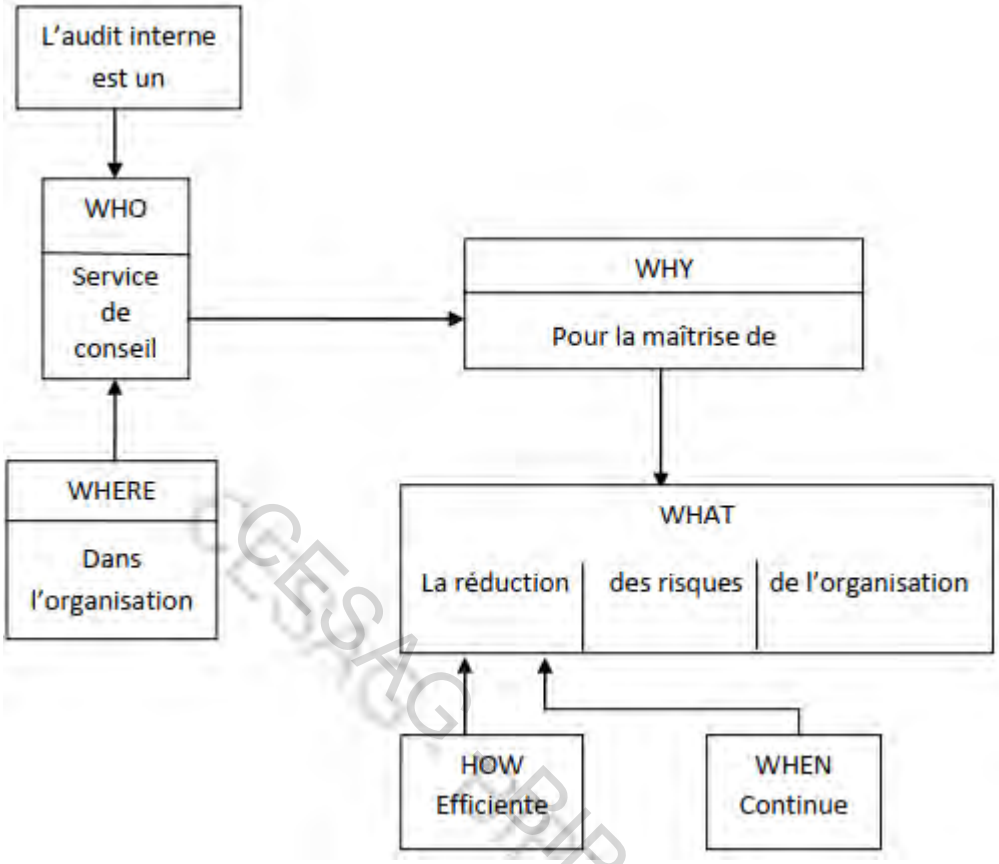
Fonction récente et évolutive, l'audit interne a vu se succéder plusieurs définitions avant que la notion ne soit stabilisée.

1.2.1.1 Notion d'audit interne

Lacolare (2010 : 10) explique que selon les normes ISO 9000 :2005 et ISO 19011 :2002, l'audit est défini comme un processus méthodique, indépendant et documenté permettant d'obtenir des preuves d'audit et de les évaluer de manière objective pour déterminer dans quelle mesure les critères d'audit sont satisfaits. En plus de lui, plusieurs comités et organismes ont tenté de donner une définition à l'audit interne. Cependant ils s'accordent tous sur cette définition de l'IIA, approuvée par l'IFACI le 29 juin 1999 : « L'Audit Interne est une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée. Il aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle, et de gouvernement d'entreprise, et en faisant des propositions pour renforcer leur efficacité. » Cette définition implique l'Audit Interne dans la fonction de conseiller, de perfectionniste, d'améliorateur. Son rôle est d'assurer la bonne santé de toutes les fonctions au sein même de l'organisation. L'audit interne est le mieux à même d'alimenter le conseil d'administration et la direction générale en informations sur les faiblesses du système de contrôle interne ou sur les zones de risques susceptibles de nuire à l'atteinte des objectifs stratégiques, opérationnels, informationnels et de conformité (Bertin 2007 : 25 – 26).

Selon CAPURSO (2001 :25) « l'audit interne est un service de conseil pour la maîtrise de la réduction efficiente et continue des risques de l'organisation ». A cet effet, le logigramme de construction ci-dessous retrace plus clairement sa définition.

Figure 1 : logigramme de l'audit interne



Source : Tommaso (2001 : 27)

1.2.1.2 Missions, objectifs et champs d'application de l'audit interne

L'audit interne connait une évolution constante du fait des changements réguliers de l'environnement dans lequel il est employé. En fonction de la définition de l'audit interne, nous ferons ressortir ses missions, ses objectifs et son champ d'application pour une meilleure compréhension de son rôle au sein de l'entreprise.

1.2.1.2.1. Les missions

Selon l'IFACI, l'audit interne présente 3 missions : Contribuer à la création de valeur ajoutée : selon l'IFACI (CRIPP 2013 : 72), l'audit interne apporte de la valeur ajoutée à l'organisation lorsqu'il fournit une assurance objective et pertinente et qu'il contribue à l'efficience et à l'efficacité des processus de gouvernement d'entreprise, de management des risques et de contrôle ; Améliorer le fonctionnement de l'organisation : par la réalisation de missions d'audit et d'apport de conseils ; Aider l'entreprise à atteindre ses objectifs : par l'évaluation des processus de management des risques, de contrôles et de gouvernement d'entreprise, à l'aide

d'une approche systématique et méthodique. Ainsi, l'Audit Interne étant une entité à part entière, doit être capable de rassurer l'entreprise sur la continuité d'exploitation, sur la maitrise des opérations (gestion des risques) et donner une garantie pas absolue mais raisonnable du succès des activités et de l'atteinte effective des objectifs.

1.2.1.2.2. Les objectifs

Dans la Modalité Pratique d'Application (MPA) 2120.A1 de l'audit interne contenu dans le CRIPP, il est spécifié les aspects sur lesquels doit porter l'évaluation du contrôle interne. Toujours dans la tendance de l'analyse par les risques, il est dit que l'audit interne doit évaluer les risques afférents au gouvernement d'entreprise, aux opérations et aux systèmes d'information de l'organisation au regard de : l'atteinte des objectifs stratégiques de l'organisation ; la fiabilité et l'intégrité des informations financières et opérationnelles ; l'efficacité et l'efficience des opérations et des programmes ; la protection des actifs ; le respect des lois, règlements, règles, procédures et contrats. Bertin (2007 : 21 – 22) pouvait dire l'audit interne est devenu un acteur majeur du dispositif de maîtrise des risques, du contrôle interne et de la gouvernance des sociétés. Il n'y a pas d'audit interne sans dispositif de contrôle interne. De ce fait, l'audit interne est une fonction d'appréciation et d'évaluation dont la tâche essentielle est notamment la validation et le maintien du contrôle interne. Sa mission principale est de s'assurer que les objectifs de contrôle interne s'inscrivent dans une approche globale du management des risques (COSO I et COSO II) et qu'ils sont relativement atteints. L'interprétation de la norme 2120 donnée par L'IFACI (CRIPP 2013 : 165), soutenue par Renard (2010 : 144) souligne que pour atteindre les objectifs en matière de management des risques, les auditeurs internes doivent s'assurer que : les objectifs de l'organisation sont cohérents avec sa mission et y contribuent ; les risques significatifs sont identifiés et évalués ; leurs modalités de traitement des risques sont appropriées et en adéquation avec l'appétence pour le risque de l'organisation ; les informations relatives sont recensées et communiquées en temps opportun au sein de l'organisation pour permettre aux collaborateurs, à leur hiérarchie et au conseil d'exercer leur responsabilité.

WILLIAN (2000 : 17) indique que « l'audit interne appuie le management dans la compréhension de la maîtrise des risques, aide à évaluer la technique de la gestion des risques, fournit un appui conséquent pour que la gestion des risques, le contrôle, la gestion du processus s'exécutent de manière efficace et efficiente, identifie et recommande les changements qui en découlent ». On peut ainsi se rendre compte que le but poursuivi par l'audit interne est de

seconder la direction dans l'accomplissement efficace de ses responsabilités en déterminant et en l'informant, si les contrôles garantissent ou non que :

- Les objectifs, les politiques, l'organisation, les procédures et les plans de la société sont respectés et conformes aux réglementations légales. Dans ce but, l'audit interne doit être informé des objectifs, politiques et plans stratégiques de l'organisation ;
- Les sécurités efficaces existent afin de prévenir les pertes ou les dommages qui pourraient survenir au patrimoine de l'entreprise ;
- Les états et les rapports d'activités sont fiables. Cette appréciation devra porter, entre autres choses, sur l'efficacité du contrôle budgétaire, la validité de donnés utilisées pour l'évaluation des projets et plus particulièrement sur toute statistique utilisée par la direction pour la prise de décision opérationnelle ou en matière d'investissement ;
- Un souci d'efficacité préside à l'utilisation des moyens matériels, humains et financiers (LEMANT, 1999 :89).

1.2.1.2.3. Les normes et le champ d'application de l'audit interne

Les activités d'audit interne sont conduites dans de différents environnements juridiques et culturels, dans les organisations dont l'objet, la taille, et la structure sont divers, ainsi que par des professionnels de l'audit, internes ou externes à l'organisation. Ces différences peuvent influencer la pratique de l'audit interne dans chaque environnement. Toutefois, le respect des normes pour la pratique professionnelle de l'audit interne est essentiel pour que les auditeurs internes puissent s'acquitter de leurs responsabilités.

❖ **Les normes d'audit interne**

Les normes font parties du cadre de référence des pratiques professionnelles. Elles représentent la base et le contrôle de qualité de la profession. Elles se proposent de :

- Définir les principes de base que la pratique de l'audit interne doit suivre ;
- Fournir un cadre de référence pour la réalisation et la promotion d'un large éventail d'activités d'audit interne apportant une valeur ajoutée ;
- Etablir les critères d'appréciations du fonctionnement de l'audit interne ;
- Favoriser l'amélioration des processus organisationnels et des opérations (IFACI, 2004 :5).

On distingue trois types de normes à savoir : les normes de qualification (série 1000) qui énoncent les caractéristiques que doivent présenter les organisations et les personnes

accomplissant les activités d'audit interne, les normes de fonctionnement (série 2000) qui décrivent la nature des activités de l'audit interne, ainsi que les critères permettant d'évaluer les services fournis.

Les normes de qualification et les normes de fonctionnement s'appliquent à l'audit interne en général tandis que les NMO se déclinent à des missions spécifiques telles qu'un audit de conformité, une investigation dans un contexte de fraude ou encore des travaux d'auto-évaluation du contrôle interne. Ces NMO sont assorties d'une lettre (précédée d'un point) qui définit le type d'activité auquel elles se rapportent soit, à ce jour : « A » pour audit (ou assurance) et « C » pour conseil. « Cette fonction conseil confirme la parfaite cohérence entre les normes et la définition de l'audit » (RENARD, 2010 :107).

Toutes ces normes peuvent être utilisées comme un moyen de développement ou comme la structure du système de formation. Nous allons traiter de quelques normes à titre d'exemples pour pouvoir illustrer les meilleures pratiques en audit interne :

- **La norme 1000 : Mission, pouvoirs et responsabilités**

Selon l'IIA (2017), la mission, les pouvoirs, et les responsabilités de l'audit doivent être formellement définis dans une charte, être cohérents avec les normes et dument approuvés par le conseil. La nature des missions d'assurance réalisées par l'organisation doit être définie dans la charte d'audit. S'il est prévu d'effectuer des missions d'assurance à l'intérieur de l'organisation, leur nature doit également être définie dans ladite charte.

La charte est un document qui indique l'exigence de la définition de la mission, des pouvoirs et des responsabilités de l'auditeur interne. Il s'agit d'indiquer clairement que ce document fondateur doit être le premier acte de la création d'un service d'audit interne.

- **La norme 1100 : Indépendance et objectivité.**

Selon l'IIA (2017), la fonction d'audit interne devrait être indépendante et les auditeurs internes devraient être objectifs dans l'accomplissement de leur mission. L'indépendance se manifeste par le rattachement à un niveau hiérarchique satisfaisant et doit être confirmée au conseil au moins annuellement. Le lien avec l'objectivité n'est pas innocent. De fait, il ne saurait y avoir de véritable indépendance sans objectivité. L'auditeur interne devrait éviter de se mêler à tout ce qui pourrait compromettre son jugement mais aussi, éviter des problèmes de conflits d'intérêts.

- **La norme 1220 : Conscience professionnelle**

Selon l'IIA (2017), l'auditeur interne doit évaluer et contribuer à l'amélioration des processus de gestion du risque, de contrôle et de gouvernement d'entreprise en utilisant une approche systématique et disciplinée.

« L'auditeur interne doit apporter à son travail la diligence et le savoir-faire que l'on peut attendre d'un auditeur raisonnablement averti et compétent. La conscience professionnelle n'implique pas l'infaillibilité. »

- **La norme 2010 : Planification**

Selon l'IIA (2017), « le responsable de l'audit interne doit établir une planification fondée sur les risques afin de définir les priorités cohérentes avec les objectifs de l'organisation. Il doit veiller à ce que les ressources affectées à cette activité soient adéquates, suffisantes et mises en œuvre de manière efficace pour réaliser le programme approuvé. » Cette norme demande à l'auditeur interne de concevoir un plan qui inclut l'étendu, les objectifs, le moment opportun des missions et les ressources nécessaires à la réalisation.

- **La norme 2040 : Règles et procédures**

Selon l'IIA (2017), « les auditeurs doivent avoir leurs procédures ; la responsabilité en incombe au responsable de l'audit interne ; simple application du contrôle interne à l'audit ». Cette norme demande aux auditeurs internes de concevoir des procédures en relation avec les normes qui leur permettront de pouvoir mener à bien les différentes missions qui leur seront assignés. Aussi, ces procédures doivent être contenues dans un support généralement appelé manuel d'audit permettant au service de renseigner leurs interlocuteurs sur les procédures utilisées.

- **Le champ d'application de l'audit interne**

Tout comme la technique comptable distingue les dépenses par natures et les dépenses par destination, critère de la distinction entre comptabilité générale et la comptabilité analytique, de même l'audit interne distingue un classement par objectifs (ou par nature) et un classement par destination.

RENARD (2006 :25) présente le classement par objectifs et précise que « ce classement permet de distinguer quatre niveaux d'application de l'audit interne que sont :

- L'audit de conformité/régularité qui permet de s'assurer que tous les dispositifs mis en place pour l'application des règles internes de l'entreprise et de la règlementation externe en matière de sécurité sont appliqués et fonctionnent parfaitement ;

- L'audit d'efficacité qui permet de s'assurer que les dispositifs mis en place pour maîtriser la fonction sécurité sont adéquats, efficaces et qu'il n'y a pas lieu de les modifier, d'en supprimer certains et d'en ajouter d'autres ;
- L'audit de management qui permet de s'assurer que la politique de sécurité est cohérente avec la stratégie de l'entreprise ;
- L'audit de stratégie qui permet de s'assurer que la stratégie de sécurité est en cohérence avec la stratégie des autres fonctions de l'organisation.

RENARD (2010 :42) précise également que « à l'opposé du classement par objectifs, le classement par destination distingue :

- L'audit de la fonction comptable ;
- L'audit de la fonction commerciale et logistique ;
- L'audit de la fonction production ;
- L'audit de la fonction informatique pour ne citer que ceux-là. »

En résumé, on peut se rendre compte que l'audit interne intervient dans les domaines tels que :

- L'examen et l'évaluation de l'efficacité des dispositifs de contrôle interne ;
- Le contrôle de l'application et l'efficacité des procédures de management du risque et méthodes de mesure de risque ;
- Le contrôle de la sincérité et de la fiabilité des enregistrements comptables et des rapports financiers ;
- Le contrôle des moyens de sauvegarde des actifs ;
- Le contrôle du système de mesure de risque par rapport aux fonds propres ;
- Les tests à la fois sur les opérations et le fonctionnement des procédures spécifiques de contrôle interne ;
- Le contrôle des dispositifs mis en place pour s'assurer qu'ils sont conformes aux exigences légales et réglementaires, aux codes de conduite, et à la mise en œuvre des politiques et procédures ;
- Le contrôle de la sincérité, de la fiabilité et de l'opportunité des reporting réglementaires (IFACI, 2001 :24).

1.2.1.3. Le code de déontologie

Il est d'une importance extrême et énonce des principes dont l'auditeur ne saurait s'écarter sans trahir sa mission. Il comprend les principes applicables à la profession et à la pratique de l'audit

interne, ainsi que les règles de conduites décrivant le comportement attendu des auditeurs internes. Il a pour but de promouvoir une culture de l'éthique au sein de la profession d'audit interne. RENARD (2010 :108) mentionne que « ce code est désormais placé en tête des normes d'audit interne et inclut deux composantes essentielles que sont :

- Des principes fondamentaux pertinents pour la profession et pour la pratique de l'audit interne ;
- Des règles de conduites décrivant les normes de comportement attendues des auditeurs internes. Ces règles ne sont rien d'autres qu'une aide à la mise en œuvre pratique des principes fondamentaux et ont pour but de guider la conduite éthique des auditeurs internes »

1.2.1.4. Les principes fondamentaux

Selon IIA (2017), Il est attendu des auditeurs internes qu'ils respectent et appliquent les principes fondamentaux suivants :

- **Intégrité :**

L'intégrité des auditeurs internes est à la base de la confiance et de la crédibilité accordées à leur jugement.

- **Objectivité :**

Les auditeurs internes montrent le plus haut degré d'objectivité professionnelle en collectant, évaluant et communiquant les informations relatives à l'activité ou au processus examiné. Les auditeurs internes évaluent de manière équitable tous les éléments pertinents et ne se laissent pas influencer dans leur jugement par leurs propres intérêts ou par autrui.

- **Confidentialité :**

Les auditeurs internes respectent la valeur et la propriété des informations qu'ils reçoivent, ils ne divulguent ces informations qu'avec les autorisations requises, à moins qu'une obligation légale ou professionnelle ne les oblige à le faire.

- **Compétence :**

Les auditeurs internes utilisent et appliquent les connaissances, les savoir-faire et expériences requis pour la réalisation de leurs travaux.

1.2.1.5. La gestion d'un service d'audit interne

Le service d'audit interne est davantage appréhendé comme un service de consultant interne que comme un outil de contrôle. En général, il existe une définition écrite du service de l'entreprise et un plan formalisé de son intervention. Une entreprise qui met en place un service d'audit interne avec un plan d'audit cherche en général à s'assurer de l'efficacité des méthodes, dans la remontée des informations en cas de décentralisation et dans le respect des procédures que l'on met en place en premier lieu les objectifs dudit service.

1.2.1.5.1. Les missions assignées au service d'audit interne

Le besoin d'audit continue de s'accroitre considérablement, et l'audit interne va être amené à voir son rôle progressivement renforcé et élargi. PHILIPE (2002 :42) mentionne que « l'audit interne était orienté vers les missions d'audit de régularité et de conformité ; il parait actuellement s'orienter vers le conseil qui est devenu une vocation de la fonction ».

La mission du service d'audit interne consiste à fournir des services indépendants d'assurance, de contrôle et de conseil, destinés à produire une valeur ajoutée et à améliorer le fonctionnement de l'entreprise. Il promet ainsi une culture de gestion efficace et efficiente au sein de l'entreprise et de ses services.

SCHICK (2007 :5) relève le rôle de l'auditeur n'est pas de dénoncer ou d'accuser, mais d'arbitrer les règles du jeu de l'entreprise et surtout de faire pratiquer les 3R : Rechercher, Reconnaitre, Remédier aux faiblesses de l'entreprise ». Cette fonction aide à anticiper les problèmes et se place dans une démarche vertueuse d'amélioration continue.

L'auditeur au sein de l'entreprise a également une mission de conseil. Cependant, RENARD (2010 :55) précise que « la mission de conseil ne devrait pas se confondre avec les recommandations des missions d'audit, lesquelles s'appuient sur des constats de dysfonctionnements. Ce sont des missions spécifiques devant être si possible définies par accord écrit ». Les services de conseil sont des activités effectuées à la demande de l'encadrement. Lors de cette mission, l'auditeur doit faire preuve d'objectivité et n'amuser aucune fonction du management.

C'est ainsi que JOUFFROY (2001 :43) affirme : « l'audit interne, dans le cadre de sa mission de contrôle, et de conseil au management contribue à minimiser où à maîtriser les risques liés à l'activité de l'organisation. Il détecte et analyse les risques, recommande les améliorations, mais en aucun cas ne les mets en œuvre ».

1.2.1.5.2. Le fonctionnement du service d'audit interne

Pour mieux appréhender ce fonctionnement, nous allons nous attarder sur quelques moyens qui doivent être mis à la disposition de ce service. Dans la réalisation de sa tâche, l'auditeur interne est en contact permanent avec les audités et d'autres personnes extérieures, d'où la nécessité d'utiliser des supports de recommandation adéquats.

1.2.1.5.2.1. La charte d'audit interne

C'est un document considéré comme l'un des plus importants car il est exigé par la première des normes professionnelles (Norme 1000). Selon LEMANT (1999 :55), « la charte est la loi fondamentale des auditeurs, qui reconnaît leur rôle et leur donne une identité. Cela explique à quoi sert l'audit, définit les règles du jeu et surtout détermine ; les pouvoirs et devoirs des auditeurs ».

La charte de l'audit interne présente quatre caractéristiques qui la singularisent par rapport aux autres documents (RENARD, 2006 :203) :

- ✓ C'est un document obligatoire : les normes professionnelles affirment que « les objectifs, les pouvoirs, et la responsabilité du service d'audit interne doivent être définis par un document officiel (charte) » ;
- ✓ La charte est le premier acte dans l'enchaînement des opérations de mise en place d'une fonction d'audit interne ;
- ✓ La charte est et doit être un document officiel : il peut s'agir d'un circulaire banal, ni d'une note d'information, ou encore moins d'un prospectif de communication ;
- ✓ La charte est un document de forme variable : il en saurait y avoir de présentation.

Ce document doit remplir quatre conditions que sont :

- ✓ Il doit être agréé et signé par la plus haute autorité de l'entreprise ;
- ✓ Il doit être distribué, et si possible, commenté, à tous les futurs audités ;
- ✓ Les références normatives qui vont lui donner une autorité extérieure, doivent y figurer ;
- ✓ Il doit être conçu dans une forme cohérente avec la culture et les habitudes de l'organisation.

La charte doit décrire le positionnement du service d'audit et de son directeur. La nature du rattachement hiérarchique de l'audit interne et son indépendance sont les principes de base posés par la déclaration des responsabilités : « le positionnement de l'audit interne doit lui permettre un exercice normal de ses responsabilités. Le responsable de la fonction doit être

rattaché à quelqu'un disposant d'une autorité suffisante pour promouvoir son indépendance, lui garantir un champ d'investigation suffisamment large et une mise en œuvre appropriée de ses recommandations. » (DIMITRIS, 2001 :54).

1.2.1.5.2.2. Le manuel d'audit interne

Tout comme la charte, le manuel d'audit interne est un document d'entreprise qui va refléter l'organisation, les habitudes de travail du service d'audit interne. Il est exigé par la norme 2040. Il a plusieurs objectifs permettant ainsi au service d'audit interne de pouvoir exercer parfaitement son rôle tout en respectant les normes qui lui sont soumises.

1.2.1.5.2.3. Le dossier d'audit

Mémoire de l'entreprise, les dossiers d'audit comprennent deux catégories de documents (RENARD, 2006 :414) :

- ✓ Des documents descriptifs : analyses des postes, organigrammes, tableau de risque, diagramme de circulation, etc. ;
- ✓ Des documents explicatifs : les feuilles d'interviews, questionnaires, FRAP (Feuille d'Analyse et de Révélation des Problèmes), tableaux de rapprochements significatifs, résultat des tests.

Les dossiers d'audit permettent de justifier et de prouver à l'égard des audités mais éventuellement à l'égard des tiers toutes les affirmations signalées dans le rapport d'audit interne. Ces justificatifs peuvent être demandés et produits soit durant la mission d'audit, soit après l'audit lorsqu'un complément d'information est sollicité durant la mise en œuvre des recommandations. Dans un cas comme dans l'autre, disposer d'un dossier complet et en ordre est un impératif absolu.

1.2.1.5.2.4. Les papiers de travail

Le papier de travail est le support obligatoire de tout constat, de toutes observations effectuées par l'auditeur interne au cours de sa mission. « Rien ne doit être laissé à la mémoire, l'auditeur est celui qui note tout » (RENARD, 2006 :416). Ces papiers de travail doivent être référencés, normalisés et comporter les indications suivantes :

- ✓ Le nom de la société auditée ;
- ✓ Désignation du service audité ;
- ✓ Le nom de l'auditeur ;
- ✓ La date de la mission.

Quand les papiers de travail se rapportent à un test, ils doivent toujours indiquer :

- ✓ L'objectif du test : en tête du document ;
- ✓ La structure du test : documents ou transactions examinés ;
- ✓ Les détails de la transaction ainsi que le résultat point par point ;
- ✓ L'interprétation des résultats en précisant le point de contrôle interne déficient ;
- ✓ Le numéro de la FRAP sur laquelle ces résultats sont analysés ;
- ✓ La référence du document, la date et les initiales de l'auditeur qui a réalisé le test.

En conclusion, de bons papiers de travail doivent toujours être :

- ✓ Normalisés ;
- ✓ Datés et Signés ;
- ✓ Compréhensibles ;
- ✓ Adéquats ;
- ✓ Simples et peu couteux ;
- ✓ Complets.

1.2.1.5.2.5. Les moyens matériels et financiers

A l'instar de beaucoup d'autres professionnels, les auditeurs internes sont appelés à travailler à distance, de manière délocalisée. Ils utilisent des moyens matériels pour :

- ✓ Une assistance à la méthodologie de travail ;
- ✓ La gestion du service d'audit ;
- ✓ L'utilisation de logiciels d'audit ;
- ✓ Le courrier électronique.

RENARD (2010 :428) préconise que « l'enveloppe financière nécessaire au service d'audit interne se détermine à partir du plan d'audit approuvé par la direction générale. Ce plan va en effet induire :

- ✓ Les effectifs et leurs variations, donc le budget rémunérations et charges de l'audit interne ;
- ✓ La formation professionnelle à dispenser aux auditeurs compte tenu de la comparaison entre les besoins exigés par les missions prévues et le profil des auditeurs en place ou à venir ;
- ✓ Les frais de déplacement qui vont être fonctions des endroits où vont se dérouler les audits prévus au plan et de la durée de ces derniers. »

A ces trois éléments qui constituent l'essentiel du budget d'exploitation, on peut ajouter :

- ✓ Les frais de fournitures et d'imprimés (en particulier documents normalisés) ;
- ✓ Des frais divers d'achats d'ouvrages et d'abonnements ;
- ✓ Des dépenses d'investissement telles que l'achat de matériels informatiques et de logiciels.

1.2.1.5.2.6. Le plan d'audit

« Le plan d'audit est un document élaboré par le service d'audit interne et approuvé par la direction générale qui indique, selon un calendrier prévisionnel de réalisation, la liste des missions à effectuer et les auditeurs qui seront en charge » (VAURS, 2000 :42).

Le plan d'audit permet ainsi d'assurer une planification du travail pour respecter l'esprit de rigueur et de méthode qui caractérise l'audit interne. Il établit à partir d'une cartographie des risques et permet ainsi de définir de façon efficace la stratégie d'audit. Il est exigé par la norme 2010 : « le responsable de l'audit interne doit établir une planification fondée sur les risques afin de définir les priorités cohérentes avec les objectifs de l'organisation. »

Le plan de l'audit doit avoir un contenu exhaustif qui comporte tous les sujets susceptibles d'être audités. Cela nécessite une démarche étalée sur plusieurs années au cours desquelles on va successivement l'enrichir, le compléter et le mettre à jour. Dans le souci de couvrir l'ensemble, le contenu du plan se fait en se basant sur plusieurs types d'approche :

- ✓ Approche par les métiers ;
- ✓ Approche par les fonctions ;
- ✓ Approches par les thèmes ;
- ✓ Approche par les processus.

De nos jours, c'est la démarche d'appréciation des risques et l'étalement des missions qui est le plus utilisé pour l'élaboration du plan d'audit.

1.2.1.5.2.7. La cartographie des risques

DUMAS (2003 :41) définit le risque comme étant « la menace qu'un évènement ou une action ait un impact défavorable sur la capacité de l'entreprise à réaliser ses opportunités ».

La cartographie des risques est un outil scientifique qui permet de connaître et de rendre compte de l'aléa, mais aussi qui permet :

- ✓ De classer, de comparer et de hiérarchiser les risques entre eux ;

- ✓ De mettre en place des plans d'actions pour les gérer en fonction des ressources disponibles ;
- ✓ D'en assurer le suivi ;
- ✓ De communiquer les informations sur les risques de l'organisation.

Selon BERGERET (2002 :32), la cartographie des risques a pour objectif :

- ✓ D'inventorier, évaluer et classer les risques de l'entreprise ;
- ✓ D'informer les responsables afin que chacun soit en mesure d'adapter le changement de ses activités ;
- ✓ De permettre à la direction générale et avec l'assistance du risk manager, d'élaborer une politique de risque qui va s'imposer à tous ;
- ✓ De permettre l'établissement du plan d'audit ;
- ✓ De favoriser l'établissement du plan d'action de gestion.

1.2.2. Cadre conceptuel de la gouvernance des systèmes d'information

Pour mieux comprendre le cadre conceptuel de la gouvernance des systèmes d'information, nous donnerons d'abord un aperçu de la gouvernance des organisations. Ensuite nous parlerons du cadre conceptuel de la gouvernance des systèmes d'information.

1.2.2.1 De la gouvernance des organisations à la gouvernance des SI

Selon KURT F. REDING & PAUL J. SOBEL « La gouvernance de l'organisation, qui constitue le niveau le plus élevé de gouvernance, est définie dans les *Normes internationales pour la pratique professionnelle de l'audit interne* comme étant : « Le dispositif comprenant les processus et les structures mis en place par le Conseil afin d'informer, de diriger, de gérer et de piloter les activités de l'organisation en vue de réaliser ses objectifs ». La gouvernance des SI est un domaine de la gouvernance de l'organisation. Elle comprend la direction, les structures organisationnelles et les processus qui garantissent que les systèmes d'information soutiennent la stratégie et les objectifs de l'organisation. La gouvernance des SI soutient les exigences réglementaires, légales, environnementales et opérationnelles de l'organisation pour lui permettre d'atteindre ses plans et ses ambitions stratégiques. D'autres domaines de la gouvernance de l'organisation comprennent la gouvernance liée aux processus de conformité ou encore celle qui concerne les processus de performance ». (Voir figure 2).

Figure 2 : Lien entre la gouvernance de l'organisation et la gouvernance des SI.

Source : IIA (2018 : 5)

1.2.2.2 cadre théorique et conceptuel de la gouvernance des systèmes d'information

La gouvernance des systèmes d'information (GSI) relève de la responsabilité des dirigeants de l'entreprise. La GSI est une organisation pour la prise de décision et répond aux préoccupations importantes des directeurs de systèmes d'information (DSI), pour assurer, dans le temps, les évolutions nécessaires du système d'information (SI), et lui permettre de répondre à des besoins de limitation des risques, de conformité réglementaire, de création de valeur ou d'alignement. Comme un grand nombre d'activités des organisations, la GSI doit trouver une réponse outillée par l'intermédiaire des applications du SI. Bien que ces outils existent, ils ne sont jamais développés en considérant les activités de la GSI dans leur ensemble.

1.2.2.2.1. Normes et standards relatifs à la gouvernance des systèmes d'information

Dans ce point il importe d'aborder la définition d'une norme de manière générale puis de parler de la norme ISO/IEC 38500 qui se rapporte à la gouvernance des systèmes d'information.

1.2.2.2.1.1 Définition d'une norme

Une norme est un document qui définit des exigences, des spécifications, des lignes directrices ou des caractéristiques à utiliser systématiquement pour assurer l'aptitude à l'emploi des matériaux, produits, processus et services.

1.2.2.2.1.2. Définition de la norme ISO/IEC 38500

La norme ISO/CEI 38500 fournit des principes, des définitions et un modèle de bonne gouvernance pour aider les dirigeants d'entreprises à cerner l'importance de la technologie de l'information (TIC). Cette norme vise à aider tous les types d'organisations à apprécier, diriger et surveiller l'utilisation des technologies de l'information peu importe le degré d'utilisation de celles-ci. Elle comporte des pratiques de management et de prise de décision associées à l'utilisation actuelle et future des technologies de l'information. L'objectif visé par la norme est de favoriser l'efficacité, la rentabilité et la conformité de l'informatique dans toutes les entreprises en donnant aux dirigeants d'entreprises des informations et des orientations sur les modalités de la gouvernance informatique, et en établissant un vocabulaire de gouvernance informatique.

1.2.2.2.2 Référentiel Cobit

Le référentiel est un ensemble structuré de recommandations ou de bonnes pratiques.
Selon Dominique MOISAND & Fabrice GARNIER DE LABAREYRE COBIT (Control Objectives for Information and related Technology) en français(les objectifs de contrôle de l'information et la technologie concernée), est le référentiel qui présente également les objectifs de contrôles et les bonnes pratiques, et les relie aux exigences métiers. Cela concerne donc principalement le système de pilotage. Mais COBIT précise aussi comment acquérir et mettre en place des technologies, afin de les aligner avec les objectifs métiers de l'entreprise. Cela se passe bien entendu au niveau du système opérant, alors que leur surveillance se situe, elle, au niveau du système d'information.
Pour la réalisation de notre mission nous ne retiendrons que le référentiel Cobit, car il est axé sur la gouvernance des systèmes d'information qui inclus la gouvernance des technologies de l'information traité par l'ISO 38500.

1.3. État des connaissances sur l'audit de la gouvernance des systèmes d'information.

Cette partie aborde l'état des connaissances sur l'audit de la gouvernance des systèmes d'information. Pour ce faire elle devra permettre de 1) comprendre les fondements de l'audit SI et 2) la démarche de l'audit SI.

1.3.1. Définition d'système d'information

Selon A. SEMOUD et A. LAYMY « Un Système d'Information (SI) est une construction formée d'informations, de traitements, de règles d'organisation et de ressources humaines et techniques. Les ensembles d'informations sont des représentations partielles de faits qui intéressent l'institution, l'organisation ou l'entreprise. Les traitements constituent des procèdes d'acquisitions, de mémorisation, de transformation, de recherche, de présentation et de communication d'informations. Les règles d'organisation régissent l'exécution de traitements informationnels. Les ressources humaines et techniques sont ce qui est requis pour le fonctionnement du SI.

Les SIs sont formés à partir de représentations partielles de la réalité (informations, traitements, règles) qui sont mises en œuvre dans un espace informatique réalisé grâce à des ressources techniques (ordinateur, réseaux, etc.). Leur fonctionnement n'est cependant possible que grâce à des acteurs humains qui sont en interaction avec le SI. »

1.3.2 audit de la gouvernance des systèmes d'information

L'IFACI et l'AFAI stipulent dans "guide d'audit sur la gouvernance du système d'information" que : « La gouvernance par l'entreprise ou l'organisation de son système d'information est une démarche de pilotage, concernant l'ensemble des responsables et pas seulement la Direction des Systèmes d'Information(DSI), ayant pour objectifs :

- D'apporter une contribution maximale à la création de valeur pour l'organisation,
- D'aligner le système d'information sur la stratégie de l'organisation,
- D'optimiser l'utilisation des ressources,
- Et de maîtriser les risques en fonction des enjeux de l'organisation.

Cette démarche, qui est fondée sur :

- Des processus de prise de décisions,
- Des instances décisionnelles,
- Des normes et des bonnes pratiques,
- Des dispositifs de contrôle adéquats,
- Et une communication visant à assurer la transparence,

S'appuie sur un ensemble de bonnes pratiques, de natures très différentes, allant :

- De sujets opérationnels, tels que l'élaboration de contrats de services ou le management de projets,

- Jusqu'à des aspects stratégiques, tels que la contribution du portefeuille de projets au développement de l'entreprise ou de l'organisation,
- En passant par des considérations économiques, telles que la maîtrise des coûts des produits ou services fournis par l'informatique à ses clients internes.

Une bonne gouvernance par l'entreprise ou l'organisation de son système d'information, par rapport aux objectifs rappelés ci-dessus, suppose qu'il n'y ait de défaillance grave sur aucun des « 12 vecteurs », et ce quelle que soit sa nature. En effet :

- Si la disponibilité des services n'est pas assurée conformément aux termes des contrats passés avec les « métiers », la DSI aura beaucoup de difficultés à se positionner comme interlocuteur de la direction générale sur les sujets concernant l'alignement stratégique du SI,
- Si les contrats de services sont respectés, mais que les ressources SI sont affectées à des projets n'ayant que peu d'intérêt pour le devenir de l'entreprise ou de l'organisation, le SI ne sera pas vraiment contributeur à la création de valeur de l'entreprise et, à ce titre, la gouvernance du SI ne pourra pas être considérée comme performante,
- Si les coûts des produits ou services ne sont pas maîtrisés correctement, il sera très difficile non seulement de garantir à la direction générale que les ressources sont utilisées de façon optimale mais aussi de développer, avec les entités « clientes », des relations de confiance basées sur la transparence du rapport « qualité/coût » des services fournis.

L'IIA dans son œuvre intitulé "auditer la gouvernance des systèmes d'information"

La mise en œuvre de la gouvernance des SI est un élément incontournable de la stratégie puisqu'elle est fondamentalement impactée par les objectifs visant à s'assurer que les SI apportent éff ectivement de la valeur aux métiers. Un cadre de référence type en matière de gouvernance des SI s'articule autour de cinq aspects majeurs :

- Alignement stratégique – La gouvernance des SI donne une orientation stratégique aux systèmes d'information et facilite l'alignement SI – métiers au niveau des services, des projets, des objectifs opérationnels, de l'actualisation de la stratégie des SI et de l'articulation des objectifs opérationnels avec les initiatives en matière de SI.
- Management des risques – La gouvernance des SI contribue à déterminer quels processus sont en place pour assurer que les risques ont été correctement traités. En outre, elle peut donner l'assurance que le management des risques de l'entreprise prend

en compte les risques liés aux investissements SI, définit les responsabilités en la matière, comprend une méthodologie d'analyse des risques commune et des stratégies pour traiter les risques. Elle vise aussi à établir une surveillance continue des menaces, de l'occurrence et de l'impact de manière holistique.

- Création de valeur – La gouvernance des SI facilite une coordination SI – métiers conçue pour optimiser l'apport des SI dans la création de valeur métiers. Les directions métiers sont alors en mesure de piloter la création de valeur par les SI et de mesurer le retour sur investissement (ROI), l'exécution du plan tactique des SI et les bénéfices visibles pour chaque niveau de l'organisation. Par exemple, le temps de fonctionnement du système (stratégie de l'infrastructure), le degré d'automatisation dans la stratégie de développement du logiciel (SDLC- *System Development Life Cycle*), la productivité (stratégie opérationnelle), et l'impact financier (stratégie financière des SI).
- Mesure de la performance – La gouvernance des SI fournit les mécanismes de vérification du respect de la stratégie (ex : atteinte des objectifs stratégiques en matière de SI), de mesure de la performance des systèmes d'information et de leur contribution au résultat net (ex : les fonctionnalités métiers promises sont-elles eff ectives ?). Il existe d'autres moyens tels que le suivi en continuelle reporting, les procédures de suivi, l'analyse causale et la gestion des problèmes, l'étude comparative au regard des pratiques du secteur ou des normes et cadres de référence éprouvés.
- Gestion des ressources – La gouvernance des SI définit la stratégie globale de gestion et d'utilisation des ressources. Elle contribue à s'assurer que les capacités et l'infrastructure des SI sont adéquates pour soutenir les besoins actuels et futurs des métiers, les stratégies de gestion des ressources, les pratiques de gestion des ressources humaines, les manuels d'utilisateur, la séparation des tâches, le suivi du temps passé, la gestion du cycle de vie de l'infrastructure, les accords de niveau de service *(Service Level Agreement* - SLA) et des politiques d'utilisation acceptables.

L'audit interne axé sur les trois lignes de maitrises, dont la première se base sur le dispositif de contrôle interne à mettre en place, la seconde à la gestion des risques, sécurité, conformité et la troisième ligne de maîtrise, à pour responsabilité d'évaluer et de formuler des recommandations en vue d'améliorer les processus de gouvernance de l'organisation (Norme 2110– Gouvernance) pour contribuer à la prévention des défaillances de gouvernance et à l'amélioration de la performance stratégique.

En eff et, selon le modèle des trois lignes de maîtrise, le management opérationnel (DSI inclus) représente la première ligne de maîtrise. Il est responsable de la mise en œuvre et du maintien des processus et des contrôles liés au management des risques. Les fonctions de conformité et de gestion des risques représentent la deuxième ligne de maîtrise et sont responsables du suivi des risques dans toute l'organisation. L'audit interne représente la troisième ligne de maîtrise et doit donner une assurance indépendante sur le bon fonctionnement du management des risques et des dispositifs de contrôle et conseiller la direction générale et le Conseil lorsque des problèmes sont identifiés.

1.3.3 Revue de la littérature sur la démarche de l'audit de la gouvernance des SI

Selon l'IIA, la revue de la littérature sur la démarche de l'audit de la gouvernance, nous permet de retenir trois grandes phases :

- La planification ;
- La réalisation ;
- La communication.

1.3.3.1 la phase de planification

Selon l'IIA dans son ouvrage "auditer la gouvernance des systèmes d'information". Il faut commencer par la planification qui consiste à savoir, si l'organisation dispose d'une structure de gouvernance unifiée et cohérente, y compris des politiques, procédures et outils pour gérer l'environnement et contrôler les risques liés aux SI en continu pour cela il faut d'abord comprendre le contexte et l'objectif de la mission qui entraine Le responsable de l'audit interne et les auditeurs internes cherchent en premier lieu à comprendre le concept de gouvernance et les caractéristiques des processus classiques de gouvernance. Ils sont également tenus d'examiner la définition du terme « gouvernance », Les référentiels, modèles et règles de gouvernance varient selon les organisations et les juridictions. La manière dont une organisation conçoit et met en œuvre les principes d'une gouvernance efficace dépend aussi de facteurs comme sa taille, sa complexité, son cycle de vie, sa maturité, la structure de son actionnariat, et les obligations légales auxquelles elle est soumise.

Ensuite nous passons à la collecte des informations qui comprend :

- Les résultats des missions d'audit des processus de gouvernance spécifiques mentionnés ci-dessus ;

- Les problèmes de gouvernance relevés dans le cadre de missions qui n'étaient pas spécialement centrées sur la gouvernance, comme les missions concernant :
  - ✓ La planification stratégique ;
  - ✓ L'efficacité et l'efficience opérationnelle ;
  - ✓ Le contrôle interne relatif à la communication financière ;
  - ✓ Les risques liés aux systèmes d'information, à la fraude, et à d'autres domaines ;
  - ✓ La conformité aux lois et règlements applicables.
- Les résultats des évaluations des risques ;
- Les résultats des évaluations par le management (par exemple, les inspections de conformité, audits qualité, auto-évaluations des contrôles) ;
- Le travail de prestataires d'assurance externes (par exemple, des enquêteurs judiciaires, des contrôleurs des finances publiques, des cabinets d'audit externe) et des régulateurs ;
- Les travaux de prestataires d'assurance internes ou de fonctions de la seconde ligne de maîtrise (par exemple santé et sécurité, conformité, qualité) ;
- D'autres informations sur les questions de gouvernance, comme des incidents indésirables indiquant des opportunités d'amélioration des processus de gouvernance.

En plus il convient de réaliser une évaluation préliminaire des risques et de prioriser les risques en fonction de leur importance mesurée selon plusieurs facteurs de risques.

Enfin définir les objectifs de la mission qui une fois que les auditeurs internes ont complété l'évaluation préliminaire des risques et identifié les risques significatifs à évaluer pendant la mission, ils peuvent définir les objectifs de la mission. Les objectifs de la mission précisent ce qu'il est prévu de réaliser pendant la mission et devraient, par conséquent, répondre à un but précis, concis et être en lien avec l'évaluation des risques (Normes 2210.A1).

Les auditeurs internes doivent également identifier les critères adéquats pour évaluer les processus de gouvernance, de management des risques et de contrôle au sein du domaine ou processus audité et pour déterminer si les objectifs opérationnels ont été atteints. L'identification de ces critères garantit que les objectifs de la mission d'assurance sont mesurables, réalistes et en cohérence avec les objectifs de l'organisation et du domaine ou processus audité.

Conformément à la Norme 2210.A3, les auditeurs internes doivent s'informer sur l'existence de critères établis par le management et/ou le Conseil. S'ils existent, ils doivent les utiliser. Si

aucun critère n'a été défini, les auditeurs internes doivent identifier, à travers une discussion avec le management et le Conseil, les critères d'évaluation appropriés. Les auditeurs devraient également envisager d'obtenir l'avis d'experts afin de développer les critères pertinents.

Exemples de critères :

- Les indicateurs clés de performance en place ;
- Les objectifs fixés pendant la planification stratégique ;
- Le degré de conformité avec les règles et procédures du domaine ou processus, les lois et règlements externes et/ou des contrats ;
- Les normes ou références du secteur.

1.3.3.2 la phase de réalisation

Selon le CIGREF, l'IFACI et l'AFAI dans l'ouvrage "guide d'audit de la gouvernance des systèmes d'information". Il faut procéder au choix de vecteurs selon le niveau de gouvernance de l'entreprise (appréciation faite par l'auditeur) ces vecteurs au nombre de 12 sont regroupés en trois domaines :

- Management
  - ✓ Planification du SI et intégration dans le plan stratégique de l'entreprise ;
  - ✓ Urbanisme et architecture d'entreprise au service des enjeux stratégiques ;
  - ✓ Gestion du portefeuille de projets orienté création de valeur pour les "métiers" ;
  - ✓ Management des risques SI en fonction de leurs impacts "métiers"
- Opérationnel
  - ✓ Alignement de la fonction informatique par rapport aux processus "métiers" ;
  - ✓ Maîtrise de la réalisation des projets en fonction des enjeux "métiers" ;
  - ✓ Fourniture de services informatiques conformes aux attentes clients ;
  - ✓ Pilotage des services externalisés.
- Support
  - ✓ Contrôle de gestion informatique favorisant la transparence ;
  - ✓ Gestion prospective des compétences informatiques ;
  - ✓ Gestion et mesure de la performance du SI ;
  - ✓ Gestion de la communication.

NB : ces vecteurs se rapportent à la norme Cobit 5.

1.3.3.3 la phase de communication

Selon l'IIA dans son ouvrage "auditer la gouvernance des systèmes d'information", le style et le format de la communication des résultats de la mission varient selon les organisations et devraient tenir compte des lois et règlements, de la culture de l'organisation et des politiques de communication, ainsi que des attentes de la direction générale et du Conseil ou des instances de gouvernance équivalentes.

Parce que la gouvernance des SI est un élément stratégique pour toute la structure de gouvernance d'une organisation, il est important que le responsable de l'audit interne communique les résultats des audits de gouvernance des SI à la direction générale, au Conseil et au comité d'audit afin qu'ensemble, ils puissent traiter toute faiblesse apparente dans le cadre de l'exercice de leurs responsabilités respectives. La Norme 2060 – Communication à la direction générale et au Conseil stipule qu'il incombe au responsable de l'audit interne d'inclure dans cette communication les enjeux significatifs en matière de risques et de contrôle, dont les questions de gouvernance nécessitant l'attention de ces organes. La gouvernance des SI est essentielle à la structure et à la stratégie de toute l'organisation et les décideurs au plus haut niveau doivent être tenus informés lorsqu'ils envisagent l'incidence stratégique de la gouvernance des systèmes d'information pour toute l'organisation.

La gouvernance des SI vient en support des exigences réglementaires, légales, environnementales et opérationnelles de l'organisation permettant la réalisation des plans et des ambitions stratégiques. Aussi, est-il impératif que la direction générale, le Conseil et le comité d'audit soient informés en temps utile des résultats des missions d'audit de la gouvernance des SI.

La démarche de l'audit est une approche collaborative qui vise l'exhaustivité. Elle parait moins réaliste qu'un test. Cependant, elle permet à l'auditeur de passer aux peignes fin le système afin de faire ressortir le maximum de détail possible.

Dans le chapitre suivant, nous présenterons les méthodes et outils qui ont servi à mener l'audit de la gouvernance des systèmes d'informations.

CHAPITRE 2 : Méthodologie de recherche

En vue de faciliter l'exploitation de la partie pratique de notre étude, il convient de présenter la méthodologie que nous envisageons utiliser. Pour ce faire nous allons procéder à l'élaboration d'un modèle d'analyse et à la justification des outils de collecte et d'analyse de nos données choisis

2.1. Le modèle d'analyse

En générale, l'audit formule des recommandations pour la résolution des difficultés de la mise en œuvre et d'application de processus. De notre point de vue l'affirmation nous semble juste car l'approche par les risques adaptés par l'audit vise l'identification et l'évaluation de tous les risques qui pourraient affecter les processus. Ces risques sont examinés, évalués et des mesures concrètes et réalisables sont proposées.

Notre approche consiste avant tous à dérouler une mission d'audit du processus du système de gouvernance des SI. Ensuite nous procéderons à une étude critique de la mission sur les points d'améliorations décelés.

Pour faciliter la compréhension de notre approche dans le cadre pratique de notre étude, nous avons adopté un modèle d'analyse (voir tableau 1). L'adoption de cette approche passe par la mise en place d'un modèle d'analyse, avant la mise en œuvre des outils techniques.

Tableau 1 : modèle d'analyses

phases	Composantes	Etapes	Outils/techniques
Planification de la mission	-prise de connaissance générale ; -orientation de la mission ;	-études documentaires ; -décomposition en objets auditables (choix des vecteurs[3]) ; -prise de connaissance des risques et opportunités d'amélioration suivant les vecteurs critiques. -analyse des risques apparents suivant les vecteurs choisis.	-revue des documents ; -interviews ;

[3] Selon l'IIA pour réaliser l'audit de la gouvernance SI. Il faut le départager en trois domaines qui sont :
1)le domaine management
2)le domaine support
3)le domaine opérationnel
Chacun de ces domaines est constitué d'un certain nombre de vecteurs qui sont mieux décrits par la suite.

Exécution de la mission	Evaluation du contrôle interne	-prise de connaissance des processus (vecteurs) ; -test de conformité suivant les différents vecteurs. -Contrôle de la conformité des processus (vecteurs) ; -évaluation préliminaire ;	-analyse organigramme ; -analyse manuelle de procédure ; -questionnaire de contrôle interne ; -interview (voir annexe 1). -Rapprochement ; -observation physique ;
Production des rapports	Formalisation des constats d'audit	-évaluation des non-conformités ; -recommandations	Feuille de révélation d'analyse de problèmes (FRAP)

Source : nous même

2.2. Outils et techniques de collecte et de diagnostic des données

Les auditeurs disposent de différents outils pour mener à bien la mission d'audit. Bien qu'il existe des méthodologies et de nombreux outils à la disposition de l'auditeur c'est son jugement et son professionnalisme qui vont déterminer, à tout moment, l'étendue des travaux à mettre en œuvre et à superviser ainsi que les outils les plus adéquats à chaque phase et pour chaque objectif.

2.2.1. Outils de collecte de l'information

Cette catégorie d'outils est utilisée tout au long de la mission et comprend les outils suivants :

- L'entretien ;
- L'observation physique ;
- Les questionnaires ;

2.2.1.1. L'entretien d'audit

L'entretien d'audit comprend différentes étapes :

- La préparation de l'entretien ;
- L'entretien à proprement parler ;

2.2.1.1.1 La préparation de l'entretien

Elle a lieu, évidemment, avant la rencontre avec la personne avec qui l'entretien sera réalisé. La préparation consiste à :

- Prendre rendez-vous : ceci permet de s'assurer de la disponibilité de l'interlocuteur. Il est préférable de prévoir une heure de début et de fin ;
- « Connaître » son interlocuteur : collecter les informations pertinentes sur cette personne dans le contexte professionnel, c'est à dire ses fonctions, sa position hiérarchique, l'information qu'il pourrait détenir et fournir, etc.
- Préparer son sujet et ses outils : lire et comprendre l'ensemble des éléments inclus dans le dossier permanent se rapportant au sujet de l'entretien ; fixer les objectifs à atteindre ; prévoir un guide d'entretien.

Dans le cadre pratique nous avons pris attache avec le responsable de la structure informatique, afin de mettre en place un planning de travail et ce planning se faisait au jour le jour par des appels téléphoniques. Au premier rendez-vous le responsable informatique nous a reçu à l'une des réunions et nous a présenté à ses collaborateurs en tant qu'auditeur qui devait travailler sur la gouvernance des SI. Après la connaissance des interlocuteurs nous avons collecté auprès d'eux un certain nombre d'information, (niveau de compétence, niveau de sécurité des SI, l'infogérance…). Enfin nous avons compris où orienter nos diligences donc le choix des vecteurs sur lesquels sera basé notre audit.

2.2.1.1.2 L'entretien à proprement parler

Il est recommandé de :

- Se présenter, si nécessaire (première rencontre avec l'interlocuteur), préciser le but de l'entretien (ceci permettra à votre interlocuteur de juger quelle information pourrait vous être utile) et confirmer la durée prévue ;
- Se concentrer sur le processus et sur le contenu ;
- Ecouter attentivement, demander l'illustration des dires par des exemples, s'assurer de comprendre ce que dit l'interlocuteur : résumer ou reformuler, de temps en temps, les informations recueillies ;
- Recentrer la discussion si nécessaire (si elle s'éloigne du but de l'entretien) ;
- Rester neutre (même si l'interlocuteur sollicite l'avis de l'auditeur) ;
- Prendre des notes, ce qui permet de : ralentir si nécessaire le flux d'information
  Conserver une trace du déroulement de l'entretien et des points essentiels
  Évoqués ;
- Varier la forme des questions : ouvertes ou fermées, alternatives, suggestives, factuelles (qui ? quoi ? où ? comment ?). Ceci contribue à maintenir l'attention de l'interlocuteur et à lui éviter l'ennui ;

- Remercier l'interlocuteur en lui indiquant que l'équipe d'audit pourrait, éventuellement, avoir des questions complémentaires par la suite.

Lors de notre entretien nous nous sommes présentés en tant qu'auditeur IT qui doit travailler sur la gouvernance des SI, nous avons pris le soin de leur dire que l'objectif de notre mission était de mettre en évidence surtout et après faire des propositions basées sur les risques auquel était confrontée la gouvernance des SI de la SIR.

Ensuite nous nous sommes intéressés sur un certain nombre de processus tel que : le processus de sécurité, le processus de communication de la structure SI d'avec les différents services métiers…

Nous sommes restés neutre, tout en posant des questions comme : qui est chargé de la sécurité du SI, qui fait la maitrise d'ouvrage des applications informatique pour les développements externes, existe-t-il un chef de projet pour chaque application à développer ?

Enfin nous les remercions à chaque fin d'entretien et suggérions leur disponibilité en cas d'éventuelles questions.

2.2.1.2. L'observation physique

Il s'agit de l'observation directe, sur le terrain de la réalisation d'une activité, le suivi d'un processus, la constatation d'une réalité. Cet outil de collecte de données sert à mieux comprendre les procédures étudiées ; il permet de suivre sur le terrain le cheminement de certaines procédures. Il permet aussi de constater si les procédures sont effectivement appliquées ou, éventuellement, les différences entre ce qui doit se faire (conception) et ce qui se fait (mise en œuvre).

Cet outil nous a permis de comprendre que la structure informatique n'avait pas une compréhension du risque de sécurité de son système d'information. Elle était fréquemment confrontée à l'indisponibilité du réseau sur l'étendue de la SIR, elle ne pouvait pas fournir d'application aux différents métiers, …

2.2.1.3 les questionnaires

Il existe différents types de questionnaires, parmi lesquels on trouve :

- Questionnaires ouverts ou fermés ;
- Questionnaire de contrôle interne ;

Parmi les bonnes pratiques pour l'utilisation de cet outil figurent :

- Adapter l'outil à l'entreprise et au secteur et garder le recul nécessaire ;

- Utiliser le questionnaire en tant que guide de l'entretien ; le questionnaire ne doit pas emprisonner l'auditeur et son interlocuteur ;
- Eviter que le questionnaire soit rempli par l'interlocuteur et qu'il se substitue ainsi à l'entretien.

Nous avons élaboré des questionnaires afin de mieux cerner le niveau de contrôle interne lié à la gouvernance du système d'information de la SIR (voir annexe 1).

Pour faire notre interview nous avons donc interrogé une population de 24 personnes en grappe de 3 personnes comme le présente le tableau 2.

Tableau 2 : grappe pour réalisation de l'interview

Secteurs	Cadres/contrmaitres	Agent technique
Direction production	7	3
Direction Finance et Gestion	9	7
Service Informatique	10	14
Direction Ressource Humaine	5	3
total	31	27
	58 personnes	

Source : nous même

2.2.2. Les outils de diagnostic

Les outils de diagnostic sont utilisés surtout, mais non exclusivement, pendant la phase de prise de connaissance de l'entité auditée et celle de l'évaluation du contrôle interne. Ces outils permettent :

- De situer l'activité, son contexte et son évolution et donc comprendre l'impact que peut avoir le contexte sur le mode d'exécution de l'activité et comment ces aspects changent au cours du temps ;
- D'évaluer les enjeux et les risques en procédant à :
    - Apprécier les seuils de signification ;
    - Etablir des comparaisons dans le temps et dans l'espace ;
    - Repérer les tendances, les variations anormales ou atypiques.

Les techniques utilisées sont :

- Décomposition de l'information (pour en réduire la complexité et étudier séparément les diverses composantes) ;
- Recherche d'indice ;
- Utilisation de ratio d'analyse financière (en considérant les tendances) ;

- Contrôle de vraisemblance (vérifier qu'une donnée n'est pas improbable, par exemple à la lumière de données similaires correspondant à des exercices antérieurs, d'un ordre de grandeur, ou des données du secteur) ;
- Examen analytique.

L'examen analytique peut être défini comme étant « un ensemble de techniques visant à faire des comparaisons entre les données figurant dans les états de synthèse et des données antérieures et prévisionnelles de l'entreprise, faire des comparaisons entre les états de synthèse de l'entité et des données d'entreprises similaires, analyser les fluctuations et tendances, étudier et analyser les éléments ressortant de ces comparaisons ».

Ces techniques permettent d'évaluer le contrôle interne et les « risques de contrôle » à travers, le plus souvent, le questionnaire de contrôle interne structuré par section des états financiers ou par cycle d'activité. Il s'agit, alors, pour chaque objectif d'évaluation, de répondre à des questions préétablies qui explicitent les principaux contrôles que devrait comporter la procédure.

Ces questions servent de guide à l'auditeur, mais ne sont jamais exhaustives. Elles permettent à l'auditeur :

- De s'assurer de la qualité de l'évaluation du système (guide et document de synthèse) ;
- D'améliorer l'efficacité de la vérification ;
- De permettre facilement la revue de l'évaluation des procédures par le responsable de mission ;
- D'améliorer les services rendus par l'auditeur aux dirigeants de l'entreprise, en mettant en évidence les faiblesses du contrôle interne.

Dans cette étape nous avons effectué notre audit sur 10 vecteurs parmi les 12 vecteurs énumérés plus haut car jugés critiques dans le cadre de notre mission. A partir de ces dix vecteurs nous avons listé les constats sur la FRAP.

2.2.2.1 Le rapprochement

C'est une technique de validation permettant de confirmer la véracité d'une information. En confrontant deux employés différents les rapprochements ont été réalisés entres les documents utilisés et les réalités sur le terrain.

2.2.2.2. La feuille de révélation et d'analyse de problème (FRAP)

Les constats d'audit ont été portés sur les feuilles de travail sous formes de FRAP. La particularité de ces FRAP est qu'elle porte des diligences dont la mise en œuvre a conduit aux constats.

Dans cette partie nous avons présenté les outils et les méthodes qui nous permettrons de découvrir les failles liées à la gouvernance des systèmes d'information, auxquelles est confrontée la SIR. Le chapitre suivant nous permet de présenter les résultats trouver, enfin faire des recommandations.

DEUXIEME PARTIE : CADRE PRATIQUE DE L'AUDIT DE LA GOUVERNANCE DU SYSTEME D'INFORMATION DE LA SIR.

Divers secteurs d'activités dans le monde des affaires actuel présentent des systèmes d'information dûment automatisés. Notre étude s'est portée sur le secteur du pétrole car celui-ci est géré au sein d'une plateforme de hautes technologies de l'information. Il en est ainsi à cause de la multitude d'information que requiert l'activité pétrolière au sein de la société elle-même et dans sa corrélation avec ses partenaires.

Ainsi l'activité pétrolière repose entièrement sur la confiance, et il ne peut y avoir de confiance sans maitrise de risques. Il n'y a pas non plus d'activité pétrolière, sans prise de risques. Les sociétés de raffinage engendrent principalement divers risques. Prendre donc l'exemple de la SIR pour effectuer notre étude nous permet d'apprécier l'implémentation et la gestion du système d'information. La Société ivoirienne de raffinage Côte d'Ivoire est par ricochet la cible de notre étude à cause de sa constante évolution et de la place importante qu'elle occupe aujourd'hui sur le plan international.

La présentation de la SIR se fera avec le chapitre 3 et dans le chapitre 4 nous ferons l'audit et proposerons des recommandations.

Chapitre 3 : Présentation de la SIR

Ce chapitre se consacre à la présentation de la société SIR, société au sein de laquelle nous avons effectué notre stage. Nous ferons l'étude de l'existant du système informatique pour mieux cerner les éléments critiques et d'y consacrer l'attention nécessaire au cours de notre mission.

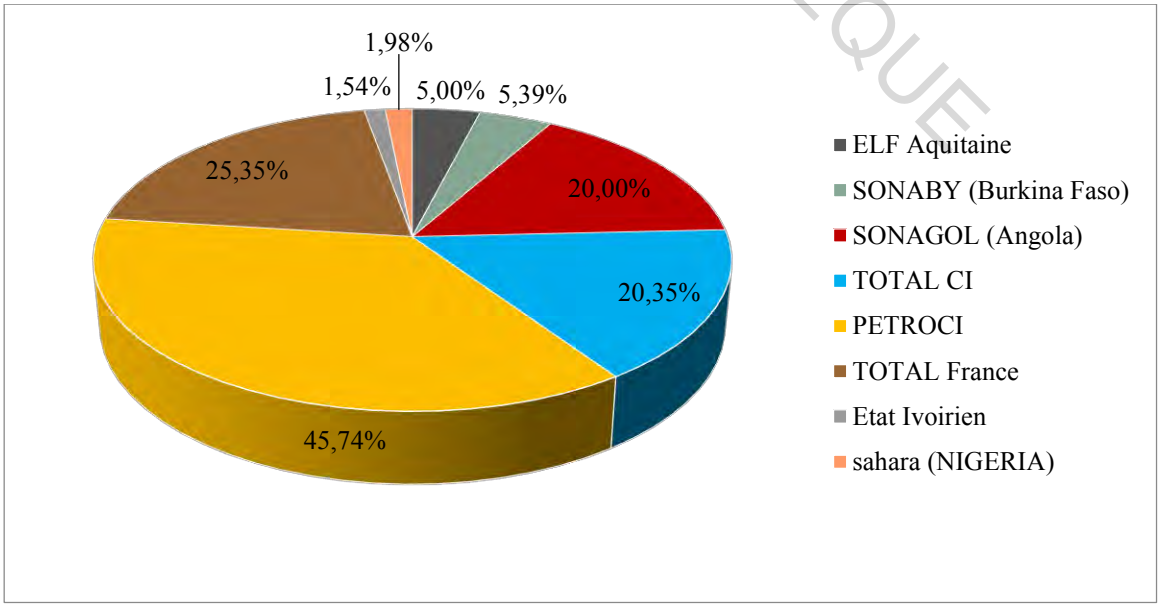
3.1. Présentation générale de la société d'accueil

La présentation de la société d'accueil tiendra compte de l'historique, des objectifs, de la mission, de l'activité, de l'organisation et fonctionnement.

3.1.1. Historique

La société Ivoirienne de Raffinage (SIR) est une société anonyme située dans la zone industrielle de Vridi à Abidjan (Côte d'Ivoire). Elle a été créée le 03 octobre 1962 par le gouvernement ivoirien avec le concours de grands groupes pétroliers internationaux, notamment SHELL et TOTAL. Elle a effectivement débuté ses activités en aout 1965 avec un capital de 20 millions de F CFA. Au démarrage, la raffinerie s'étendait sur une superficie de 40 hectares avec une capacité de traitement de 700.000 tonnes de brut par an. Aujourd'hui, la SIR a beaucoup progressé. Sa superficie est estimée à 80 hectares avec une production annuelle de 3.800.000 tonnes par ans. Son capital actuel s'élève à 39 milliards de F CFA et est reparti comme suit :

Figure 3 : part des différents actionnaires



Source : GRH SIR (2019)

La SIR dispose de deux unités HYDROSKIMMING (HSK2 et HSK3) qui sont des unités de distillations atmosphériques permettant le fractionnement du pétrole pour l'obtention des sous-produits, notamment l'essence, le kérosène, le gasoil lourd, le gasoil léger et les résidus atmosphériques. Son dispositif comprend aussi un hydrocraqueur (DHC), instrument de haute technologie, conçu pour la transformation du résidu atmosphérique. Avec cette unité, il n'y a pas de résidu à éjecter « 100%brut, 100% produits finis. »

3.1.2. Objectifs

Pour faire face à la mondialisation et à la rude concurrence, la SIR a mis sur pied un plan stratégique dénommé « business model ». Conçu en interne, ce plan fixe des objectifs concrets et permet de mesurer les progrès accomplis. Il a pour but :

- L'amélioration de la productivité ;
- La maitrise efficace des charges ;
- L'ouverture de nouveaux marchés porteurs.

3.1.3. Missions

La SIR a pour vocation de :

- Fabriquer des produits pétroliers pour le marché ivoirien et l'exporter ;
- Assurer la sécurité de l'approvisionnement de la Cote d'Ivoire ;
- Etre une entreprise à dimension internationale, compétitive, performante, rentable et pérenne ;
- Etre une entreprise socialement responsable et respectueuse de l'environnement.

3.1.4. Activité

L'activité principale de la SIR est le raffinage du pétrole brut provenant de certains pays tels que le Nigeria, le Cameroun et la commercialisation des produits finis. Grace à sa performance et sa technicité, elle parvient à alimenter les marchés de la Cote d'Ivoire et certains pays de la sous-région.

Le tableau 3 montre les différents produits pétroliers fabriqués à la SIR et leurs différents usages :

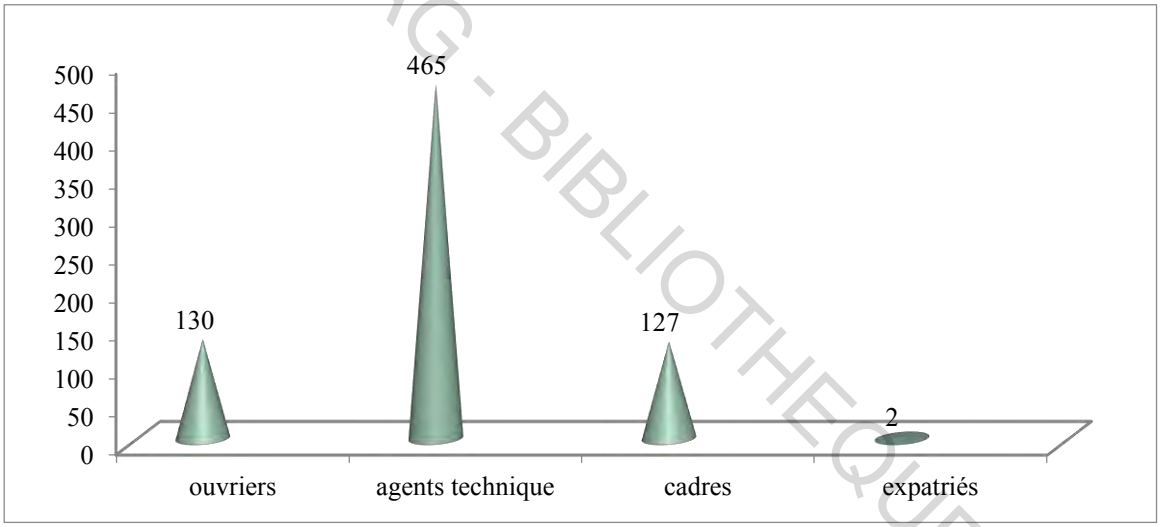
Tableau 3: produits pétrolier fabriqués par la SIR.

Produits fabriqués	utilisation	Pourcentage (%)
butane	Usage domestique	1
Essence super	Carburant automobiles, moteur à essence	5
Essence ordinaire		15
Pétrole lampant	Eclairage en milieu rural	23
Kérosène (carburateur)	aviation	
gasoil	Moteurs diesel	29
Distillate diesel oil (DDO)	Fours et diesel	5
Heavy Vaccum oil	Turbines à gaz	12
Fuel oïl 180,380 ET 450	Centrales thermique et navires	10

Source : GRH (2019)

La SIR compte à ce jour 724 agents qui se répartissent comme suit :

Figure 4 : répartition du personnel de la SIR.

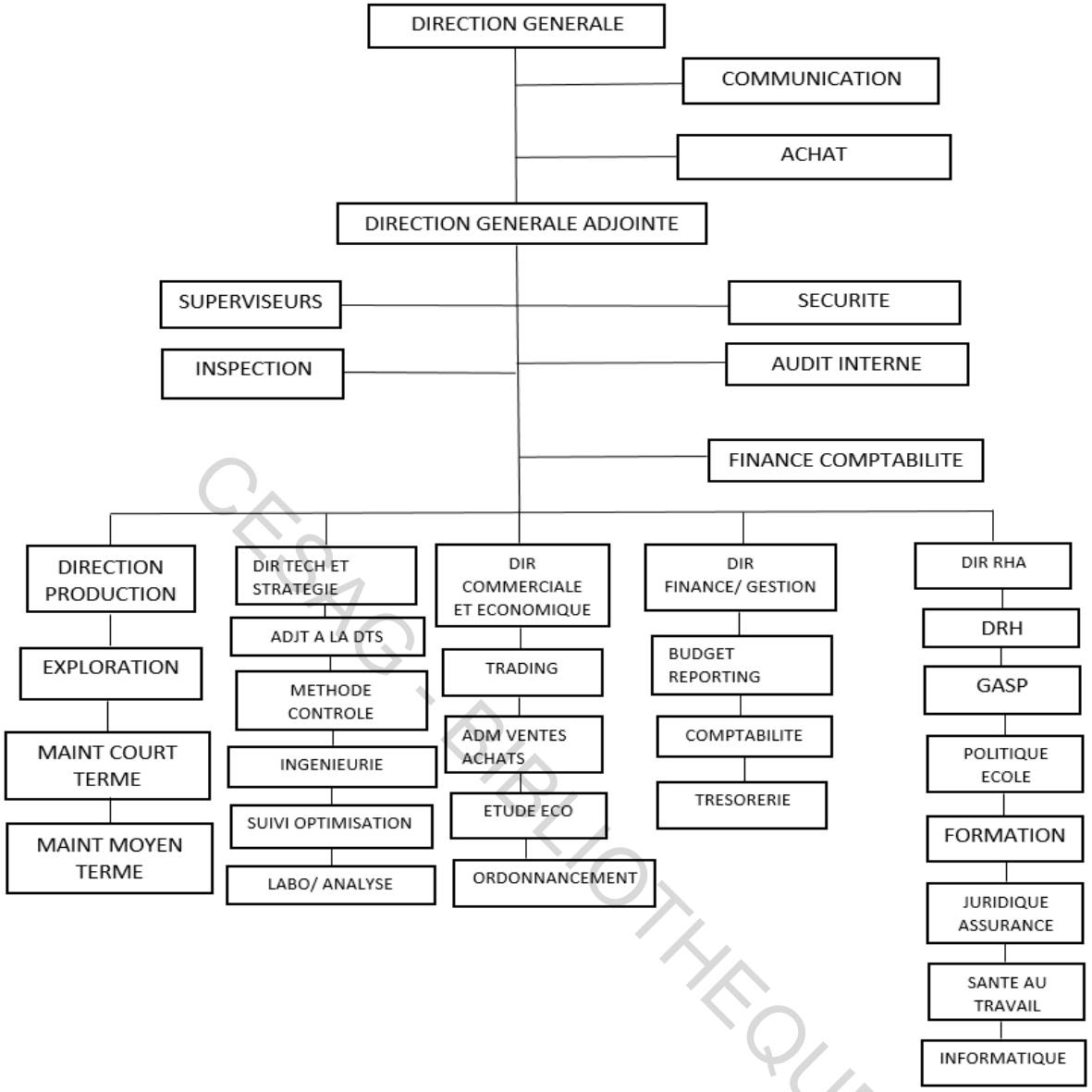


Source : GRH SIR (2019)

3.1.5. Organisation et fonctionnement

La figure 5 présente l'organigramme de la SIR :

Figure 5 : organigramme de la SIR (2019)



Source : GRH SIR (2019)

Selon qu'il est présenté ici, L'organigramme de la société ivoirienne de raffinage comprend principalement :

- Le directeur général ;
- Le directeur général adjoint ;
- Le directeur de la production ;
- Le directeur technique et stratégique ;
- Directeur commerciale et économique ;
- Directeur finance et gestion ;
- Directeur des ressources humaines et de l'administration.

- La structure informatique de gestion.

3.2. Présentation de la structure informatique

La structure informatique est dirigée par un responsable qui a la charge, de s'assurer de la disponibilité du réseau, du développement des applications et la maintenance des différents équipements.

Elle est subdivisée en deux sections :

- Section matériel, système et réseau ;
- Section étude et développement de projet.

3.2.1. Section matériel, système et réseau

Elle est une section de la structure informatique et est dirigée par le responsable matériel, système et réseau. Elle a pour mission de faire l'inventaire régulier des équipements disponibles et connectés au réseau, de faire la supervision du réseau afin de régler les cas d'indisponibilités. Il a la charge d'assurer la sécurité du réseau et l'achat de nouveau équipements.

3.2.2. Section étude et développement de projet

Le responsable est chargé de travailler sur un ensemble de portefeuille projet avec les services extérieurs à l'entreprise. Il se charge aussi de l'attribution des droits d'accès aux différents portails des applications.

Cette partie de notre travail nous a permis de présenter la SIR. Dans le chapitre suivant nous allons procéder à l'audit de la gouvernance de son système d'information.

CHAPITRE 4 : audit de la gouvernance du système d'information de la SIR

Dans ce chapitre, nous décrirons la gouvernance du système d'information de la SIR selon le référentiel cobit 5 établit par l'ISACA. Nous procéderons à l'analyse et à l'interprétation de ces résultats et également à la présentation et à l'analyse des risques dus aux insuffisances de la gouvernance des SI. Enfin nous proposerons des recommandations et des solutions idoines.

4.1. Périmètre d'audit

La délimitation du périmètre d'audit qui constitue pour nous une armada solide à l'efficacité de notre mission a été répartie comme suit : Périmètre physique : le service informatique, la direction production, la direction finance et gestion, le service achat, la structure gouvernance et contrôle interne. Périmètre logique : le réseau informatique, les différentes applications et les communications entre les différentes applications des périmètres physiques cités plus haut.

Cette partie de notre travail nous a permis d'étudier l'existant de la gouvernance du SI de la SIR.

4.2. Planification, réalisation, de l'audit de la gouvernance du SI de la SIR

L'audit de la gouvernance du système d'information de la SIR se basera sur certains vecteurs selon le référentiel Cobit 5. Ces vecteurs choisis répondent bien aux préoccupations des managers de la SIR.

4.2.1. Planification de l'audit de la gouvernance du SI de la SIR

Lors de cette phase nous avons cherché à savoir, si l'organisation dispose d'une structure de gouvernance unifiée et cohérente, y compris des politiques, procédures et outils pour gérer l'environnement et contrôler les risques liés aux SI en continu. Donc il fallait d'abord comprendre le contexte et l'objectif de la mission, comprendre le concept de gouvernance et les caractéristiques des processus classiques de gouvernance. Nous avons également tenu d'examiner la définition du terme « gouvernance », Les référentiels, modèles et règles de gouvernance de la SIR. Nous avons ensuite rencontré les responsables afin de nous imprégner la manière dont la SIR conçoit et met en œuvre les principes de gouvernance SI, son niveau de maturité en terme de gouvernance SI, et son niveau de maitrise des risques SI.

Après avoir recueillir tous ces informations nous avons situé les difficultés de gouvernance SI de la SIR sur les domaines et vecteurs de gouvernances suivants :

- Management

- ✓ Structure organisationnelle de la fonction gouvernance SI et fonctions clés ;
    - ✓ Urbanisme et architecture d'entreprise au service des enjeux stratégiques ;
    - ✓ Gestion du portefeuille de projets orienté création de valeur pour les "métiers" ;
    - ✓ Management des risques SI en fonction de leurs impacts "métiers".
- Opérationnel
    - ✓ Alignement de la fonction informatique par rapport aux processus "métiers" ;
    - ✓ Pilotage des services externalisés.
- Support
    - ✓ Contrôle de gestion informatique favorisant la transparence ;
    - ✓ Gestion prospective des compétences informatiques ;
    - ✓ Gestion et mesure de la performance du SI ;
    - ✓ Gestion de la communication.

4.2.2. Réalisation de l'audit de la gouvernance SI de la SIR

La réalisation de l'audit de la gouvernance SI de la SIR porte sur les domaines et vecteurs cités à la phase de planification.

4.2.2.1. Domaine management

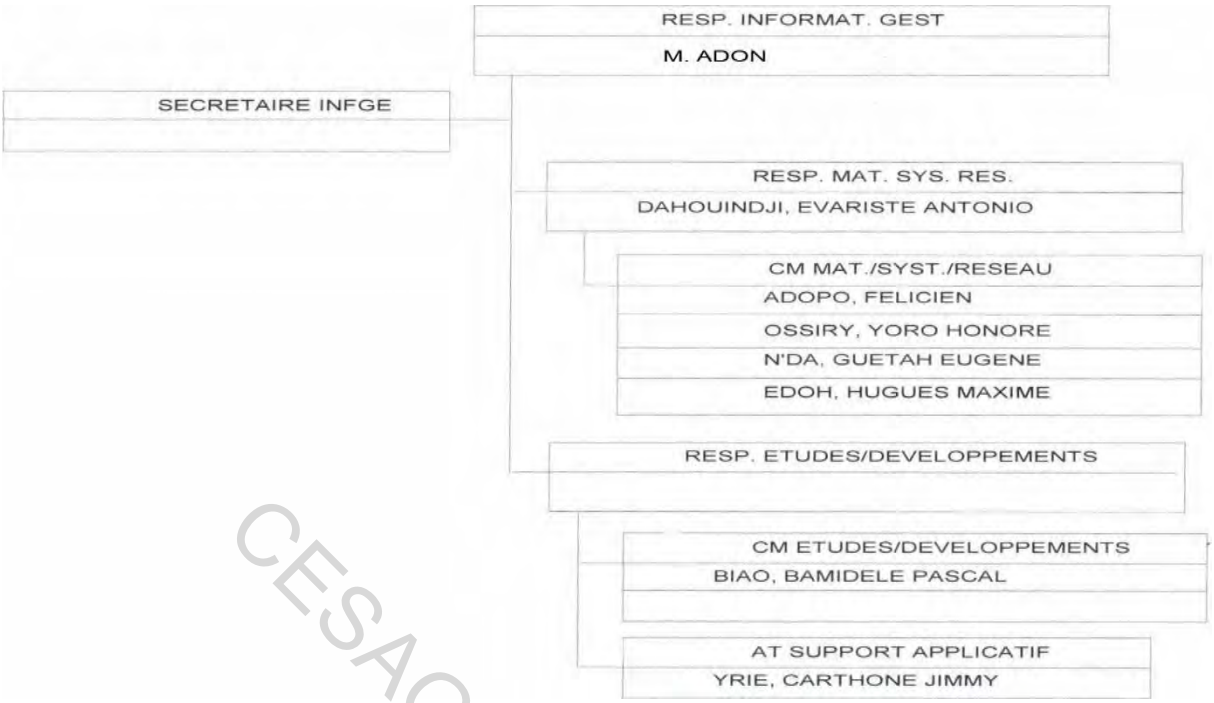
Dans ce domaine nous avons fait notre audit sur les vecteurs jugés critiques pour la SIR.

4.2.2.1.1. Structure organisationnelle de la fonction gouvernance SI et fonctions clés

❖ **Constat**

- La structure informatique de la SIR se présente sous une forme classique en majorité constitué de techniciens de maintenance et réseau comme observé à la figure 6 :

Figure 6 : organigramme de la structure informatique



Source : structure informatique (2019)

❖ Cause

La gestion des carrières n'étant pas encore de mise, donc les managers préfèrent cette structuration.

❖ Conséquences

L'insuffisance liée à la structuration de la structure informatique va entrainer des conséquences telle que :

- Le surcout dû au fait de dépenser pour l'acquisition de certains équipements et les abandonner pour quelques mois plus tard pour leur non utilité
- Le fait de ne pas attribué de responsabilité de la sécurité informatique crée du flou et laisse le réseau vulnérable vis-à-vis des pirates.
- Cet organigramme entraine le manque de confiance des différents services métiers vis-à-vis de la structure informatique.
- Obligation de trouver des consultants pour les petites taches telles que la formation des agents pour l'utilisation de SAP.

4.2.2.1.2. Urbanisme et architecture du SI de la SIR au service des enjeux stratégiques.

- **Constat**
- **Forces**
- **Description du système d'information de la SIR**

Il s'agira pour nous de décrire les différentes composantes qui participent au fonctionnement du système informatique. Après une première séance de visite guidée, nous avons observé les différentes installations et pris connaissance de leur condition d'utilisation.

- **Inventaire des micro-ordinateurs, serveurs, applications, baies**

Les micro-ordinateurs sont repartis en fonction des zones de la société. Le résumé de l'ensemble de ces équipements est présenté dans le tableau 4.

Tableau 4 : répartition générale des équipements informatique de la SIR

	Répartition générale							
	DG	DGA	DFG	DCE	DRHA	DTS	DP	TOTAL
ORDINATEURS	49	45	31	45	150	126	178	624
TABLETTES	1	2	1	3	6	4	2	19
PC PORTABLE	2	1	0	0	4	1	3	11
VIDEOS PROJECTEURS	3	1	0	0	4	2	1	11
SCANNEUR	4	1	1	2	6	6	5	25
IMPRIMANTES RESEAUX	3	3	7	5	11	16	18	63
IMPRIMANTES INDIVIDUELLES	13	13	9	7	51	27	46	166
IMPRIMANTES MULTIFONCTION	7	5	7	5	27	16	27	94

Source : structure informatique (2019)

Tableau 5 : différents Switch utilisés par la SIR.

Nbre	LTP/LTS	LOCALISATION	MATERIEL	MODELE	N°SERIE	MAC ADDR.	NBRE DE PORTS
1	LTP 1	Bâtiment administratif	SWITCH	HP Procure 5308XLJ4819A	SG343JZ027	00306eb87a00	24 Mini-GBIC
2		Bâtiment administratif	SWITCH	HP Procure 5308XLJ4819A	SG343JZ027	00306eb87a00	24 RJ45

3	LTP 2	Salle 3 AE	SWITCH	HP Procure 5308XLJ4850A	SG344JK00S	00306ab8ce00	8 Mini-GBIC5
4		Salle 3 AE	SWITCH	HP Procure 5308XLJ4850A	SG344JK00S	000D9D772D00	24 RJ45

Source : structure informatique (2019)

La SIR possède deux catégories de serveur à savoir les serveurs physiques et les serveurs virtuels qui sont énumérés dans les tableaux 6,7 et 8 :

Tableau 6 : liste des serveurs physiques de la SIR.

Nom du serveur	Marque et Modèle	OS	Rôles	Hôte de VMS
SIREXCHMBX1	HP Proliant DL 380 G5	W 2008 Server R2	Serveur de messagerie Exchange 2010	Non
SIRPDC2008R2	HP Proliant DL 380 G5	W 2008 Server R2	Contrôleur de domaine primaire 2008 R2	Non
SIRVMEDGE1	HP proliant DL380 G5	W 2008 Server Datacenter R2	Serveur de virtualisation	Oui
SIRVMEDGE2	HP proliant DL380 G5	W 2008 Server Datacenter R2	Serveur de virtualisation	Oui
SIRSTARLIMS	HP Proliant DL 380 G6	W 2003 Server	Serveur Startlims V10	Non
SIRBELSIM	HP Proliant DL 380 G5	W 2003 Server	Serveur BELSIM	Non
SIRP2IPROD	HP Proliant DL 580 G5	W 2003 Server US	Serveur de production MPRO	Non
SIRHRPRODV7	HP Proliant DL 380 G5	W 2003 Server	HR ACCESS version V7	Non
SIRVMIP21	HP Proliant DL 380 G5	W 2008 Server R2	serveur de virtualisation IP 21	Oui
SIRVM8	HP Proliant DL 560 G8	W 2012 Server R2	Serveur de virtualisation	Oui
SIRVM	HP Proliant ML 350 G5	W 2008 Server R2	Serveur de virtualisation	Oui
SIRVM4	HP proliant DL380 G7	W 2008 Server R2	serveur de virtualisation	Oui
SIRVM5	HP Proliant DL 380 G5	W 2008 Server R2	Serveur de virtualisation	Oui
SIRVM6	HP Proliant DL 380 G5	W 2008 Server	Serveur de virtualisation	Oui
SIRCLGED1	HP proliant ML 380 G5	W 2008 Server R2	Serveur de virtualisation	Oui

Source : structure informatique (2019)

Tableau 7 : liste de serveurs virtuels

Hôte	VMS	Etat	HDD	OS	Rôle	Stockage	BACKUP
SIRVM2	**SIRGESEQUIP**	**Exécution**	50	W 2003 SP2	Gestion équipements Inspection	Baie HP 4300	
	SIRSPBAS	**Exécution**	126	W 2008 R2 SP1	Test de développement SHAREPOINT	Baie HP 4300	Azure
	PCCONSULTRH	**Exécution**	148	Win 7 Entreprise	Développement RH	Baie HP 4300	Azure
	PCIGDEV2	**Exécution**	70	Win 7 Entreprise	Développement RH	Baie HP 4300	Azure
	PCMSIX64	**Exécution**	80	Win 7 Entreprise	Création Package MSI	Baie HP 4300	
	PCMSIX32	**Exécution**	80	Win 7 Entreprise	Création Package MSI	Baie HP 4300	
	SIRWEB	**Exécution**	70	W 2008 R2	Production Site internet SIR.	Baie HP 4300	Azure
	PCSTAR	**Exécution**	85	Win 7 Entreprise	Client STAR	Baie HP 4300	
	SIRPRINT2012	**Exécution**	72	W 2003 R2 SP2	Serveur d'impression	Baie HP 4300	
	SIRSPS	**Exécution**	100	W 2008 R2 SP1	Serveur SharePoint	Baie HP 4300	Azure
	SIRSQL	**Exécution**	348	W 2008 R2 SP1	serveur SQL pour SharePoint	Baie HP 4300	Azure
	PCTESTSCM1	**Exécution**	80	Win 7 Entreprise	Pc de test SCCM	Baie HP 4300	
	SIRSAPGED	**Exécution**	299	W 2008 R2 SP1	Serveur GED pour SAP	Baie HP 4300	Azure
	SIRINTRANET2	**Exécution**	292	W 2003 R2 SP2	Serveur intranet	Baie HP 4300	Azure

Source : structure informatique (2019)

Tableau 8 : baies de stockage de la SIR

	BAIES	IP	Taille (TO)	Cluster	Volume total (TO)	Hôtes	Volume hôtes (TO)	Volume sur Cluster (TO)
BAIE COMPUTEC HP 4300	BAIEADM1A	61.1.250.25	6,31	BAIE_P4300_MGT (IP : 61.1.250.210)	25	SIRCLGED1	2	2,81
						SIRDESKMGR	3,5	7
	BAIEADM1B	61.1.250.81	6,31			SIRVM2	2	4
	BAIE3AE1A	61.1.250.149	6,31			SIRVM4	1	1,89
						SIRVM5	1	1,99
	BAIE3AE1B	61.1.250.148	6,31					
						Volume Total sur Cluster (TO)		17,69

Source : structure informatique (2019)

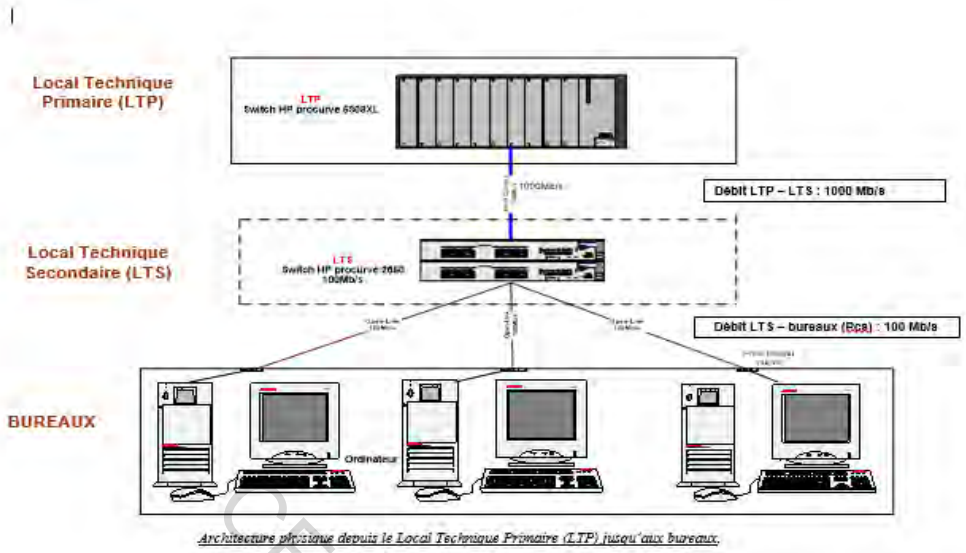
- **Architecture et topologie du réseau**

Le réseau informatique de la SIR est un réseau de type ETHERNET. Il a été mis en place en 1992, par la société DIGITAL EQUIPEMENT CORPORATION (D.E.C).

A sa création, il fonctionnait à 10 Mbits/s, puis a été porté à 100 Mbits/s (débit entre LTS et PCs). La partie principale « backbone » de ce réseau est constituée de la fibre optique. Ce réseau est articulé autour d'une topologie étoile dite « hiérarchisée », qui utilise un câblage différencié entre la partie verticale (immeuble de plusieurs étages) ou étendue (plateforme ou campus) et la partie horizontale (zone de bureaux). Le cœur de ce réseau est situé dans un local technique principal (LTP) et chacune des extrémités dans un local technique secondaire (LTS). Nous disposons de :

- deux locaux techniques principaux (LTP) avec des switches HP Procurve 5308 XL.

Figure 7:architecture physique depuis le local technique primaire jusqu'aux bureaux



Architecture physique depuis le Local Technique Primaire (LTP) jusqu'aux bureaux.

Source : structure informatique (2019)

- seize locaux techniques secondaires (LTS) avec des switches HP Procurve 2650.

A partir d'un tableau de brassage optique situé dans le local technique principal (LTP), un câble optique de dix (10) brins part à destination de chacun des locaux techniques secondaires (LTS). L'ensemble des matériels actifs (transmetteurs optiques, switches HP procurve 2650, platines de distribution) judicieusement reparti dans chacun de ces locaux techniques secondaires, permettent la distribution des réseaux capillaires paires torsadées, destinés à desservir les postes de travail en prises informatiques.

Le réseau informatique de la SIR dispose de quatre (04) topologies différentes au niveau de sa configuration. Ce sont :

- **La topologie ETOILE ACTIVE – FIBRE OPTIQUE.**

Cette topologie concentre tous les locaux techniques secondaires (LTS) en un point fixe au niveau du local technique principal (LTP). Le choix de cette topologie s'explique par le fait qu'elle permette une facilité des échanges, des connexions multiples, l'indépendance des postes de travail, et est adaptée à l'environnement de la SIR. Le câblage utilisé est la fibre optique pour sa large bande passante (quelques dizaines de mégahertz à plusieurs gigahertz), pour sa vitesse de transmission plus élevée, pour son insensibilité aux perturbations électromagnétiques et son insensibilité aux bruits de la raffinerie. La vitesse de propagation des signaux entre LTP et LTS est de 1000 Mbits/s.

Figure 8: schéma du réseau informatique de la SIR

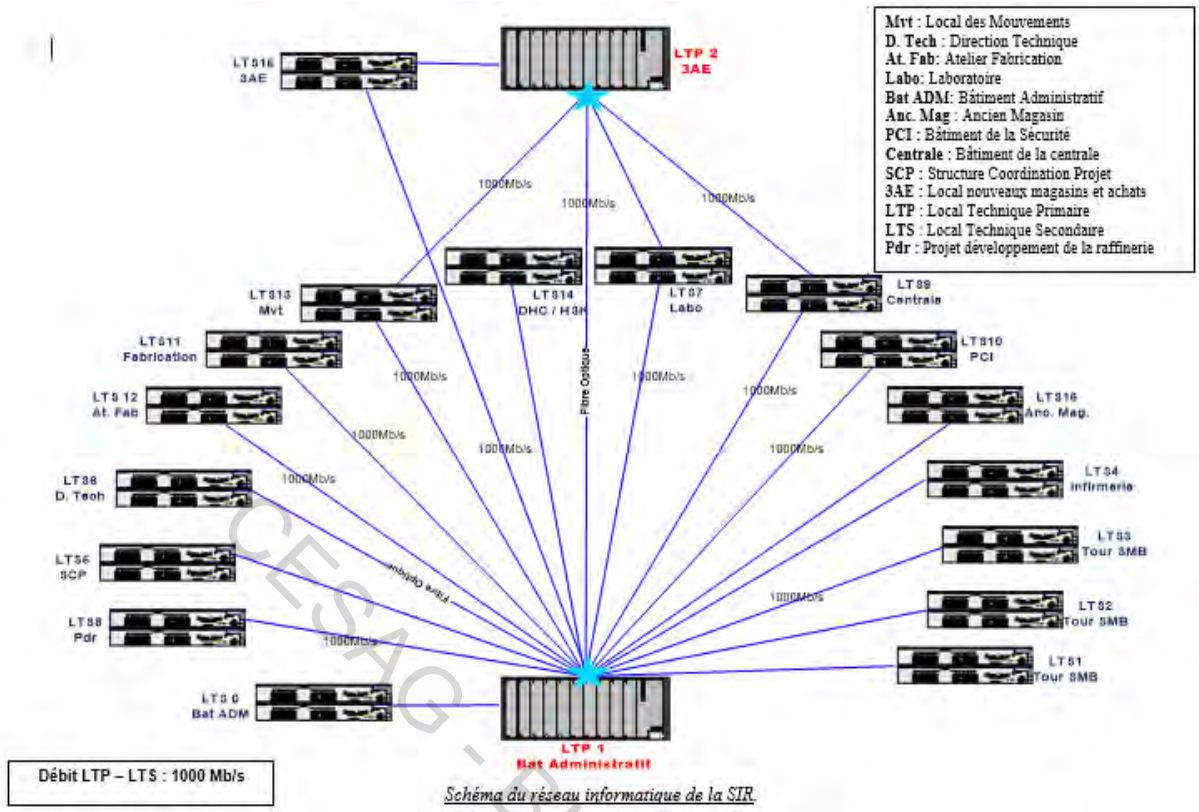


Schéma du réseau informatique de la SIR

Source : structure informatique (2019)

- **La topologie DOUBLE ETOILE ACTIVE.**

Cette topologie est particulière, car elle connecte deux locaux techniques principaux (LTP). Le câblage utilisé est la fibre optique. Le premier local technique principal est celui qui relie tous les 16 locaux techniques secondaires (LTS). Le second est non seulement connecté au premier, mais aussi à trois sites prioritaires. Il s'agit :

- du site de la CENTRALE (LTS 9),
- du site du MOUVEMENT (LTS 13).
- du site abritant l'unité HSK2 (LTS 7).

Ces sites contiennent les données les plus importantes de la raffinerie. Le second LTP a été mis au point pour secourir le premier en cas de panne de celui-ci, évitant ainsi les pertes d'informations dans les trois sites prioritaires. La passation de service entre ces deux LTP se fait de façon automatique. La vitesse de propagation est de 1000 Mbits/s.

- **La topologie ETOILE-OPEN LINK.**

Cette topologie est utilisée pour connecter les postes de travail aux locaux techniques secondaires (LTS). Elle utilise le câble Open Link de DIGITAL pour la connexion entre les LTS et les prises murales situées dans les différents bureaux.

Les câbles pairs torsadées assurent ensuite la connexion entre les prises murales et les postes de travail. Cette topologie peut connecter plus de 140 postes de travail par LTS. L'utilisation des platines de distribution et des switches HP procurve 2650 concentre les câbles Open Link sur les LTS. La vitesse de transmission des données entre un PC et le LTS étant de 100 Mbits/s.

- **La topologie DOUBLE ETOILE-OPEN LINK.**

Cette topologie concerne les trois sites prioritaires. Outre la configuration semblable à celle des autres LTS, elle dispose d'une autre configuration provenant du second LTP et à une vitesse de 100 Mbits/s.

Nous disposons de deux liaisons internet :

- **AFNET (10 MO)**
- **AVISO (8MO)**

Nous disposons de trois (03) proxys utilisant nos deux liaisons internet. Ce sont :

- **Le Proxy NEOS** (firewall, relais interne et externe) est utilisé pour la navigation internet de la majorité des utilisateurs via le fournisseur AVISO (CI-TELECOM).
- **Le proxy SIRPROXY1** permet la navigation internet d'un certain nombre d'utilisateurs via les deux fournisseurs AVISO (CI-TELECOM) et AFNET (MTN).
- **La passerelle CYBEROAM (SOPHOS) sécurisée** permet la navigation internet des utilisateurs via les deux fournisseurs AVISO (CI-TELECOM) et AFNET (MTN).

Messagerie Externe.

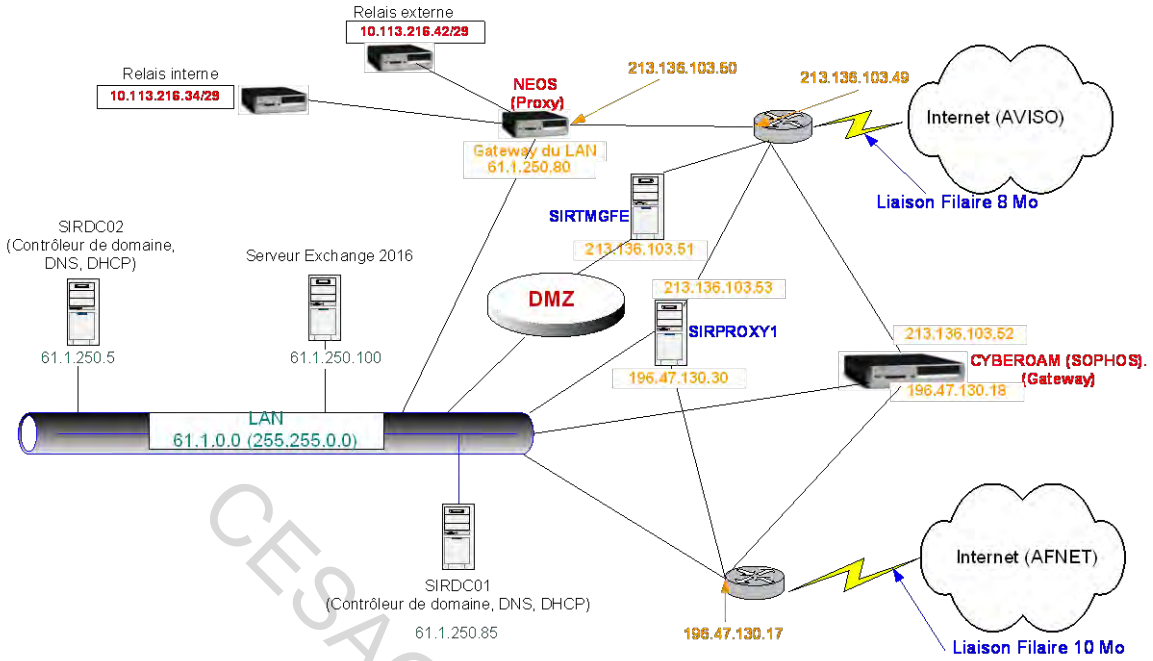
- Le serveur **SIRTMGFE** situé en regard externe est séparé de notre LAN par une DMZ. Cette DMZ contient une partie de nos serveurs Exchange (EDGE) et deux serveurs TMG, les autres serveurs Exchange (MailsBox et HubCas) étant situés sur le LAN (voir schéma de l'architecture de la messagerie SIR).
- Ce serveur **SIRTMGFE** est celui par lequel passe toute notre messagerie via l'extérieur. Nos enregistrements MX chez AVISO pointent vers l'adresse 213.136.103.51 qui n'est autre que l'adresse de la patte externe de ce serveur SIRTMGFE.

Téléphonie IP à l'international.

- La liaison AFNET est utilisée pour la téléphonie IP à l'international et aussi pour la navigation internet d'un nombre très restreint d'utilisateurs et pour l'envoi des SMS via une passerelle dénommée HYPERMEDIA SMS.

Le schéma 9 illustre bien l'architecture de notre connexion à internet.

Figure 9: architecture connexions internet SIR.



Source : structure informatique (2019)

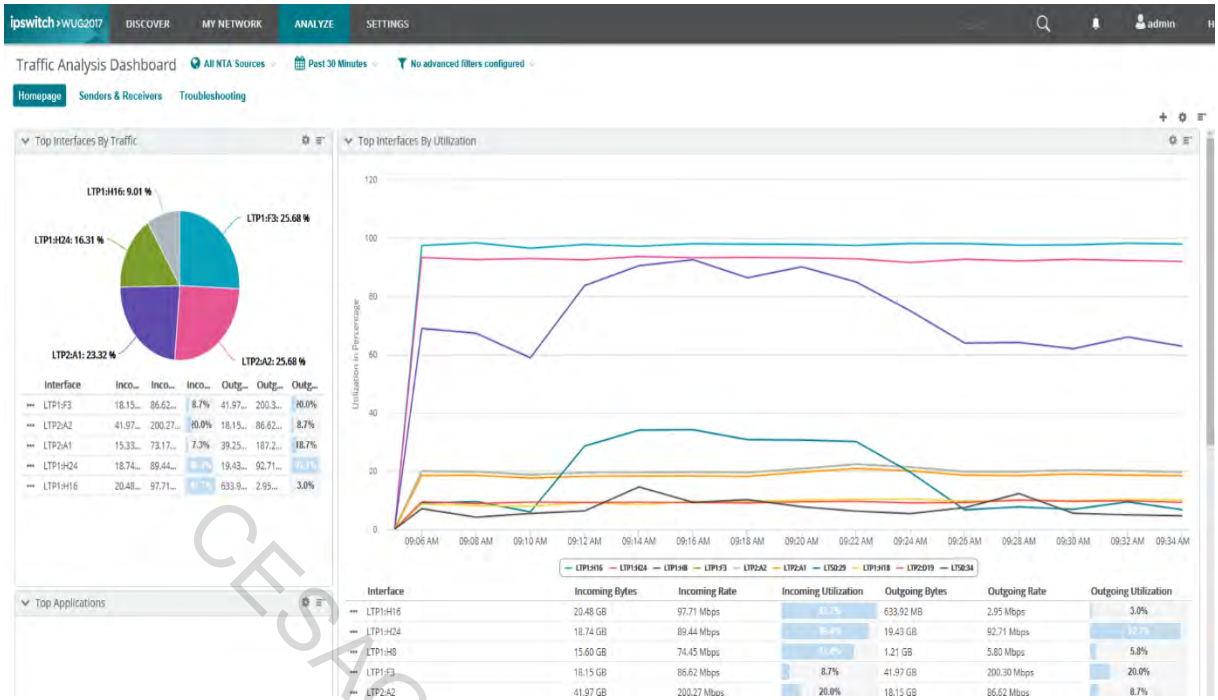
Le réseau actuel de la SIR est constitué de 624 postes appartenant à différents bâtiments interconnectés entre eux par une cascade de 28 Switches.

Le local de la SIR comporte un câblage réseau normalisé et dispose de plage d'adresse IP routables alloués au routeur et aux postes de travail connectés au réseau.

- **Faiblesses**

- Quarante-cinq plantages du réseau durant l'année 2018 ;
- Tous les switches sont obsolètes (100 Mb/s) ;
- Impossibilité d'avoir les pièces de maintenance par la vétusté des appareils réseau ;
- Tous les postes de travail connectés au réseau sont placés sur le même segment ;
- Mauvais trafic du réseau locaux techniques primaires voir figure 10.

Figure 10: trafic réseau de la SIR



Source : structure informatique (2019)

❖ Causes

- La maîtrise insuffisante de certaines technologies ;
- La complexité rendant difficile toute évolution.

❖ Conséquence

- Subir des attaques virales à n'importe quel moment.

4.2.2.1.3. Gestion de projets orienté création de valeur pour les métiers

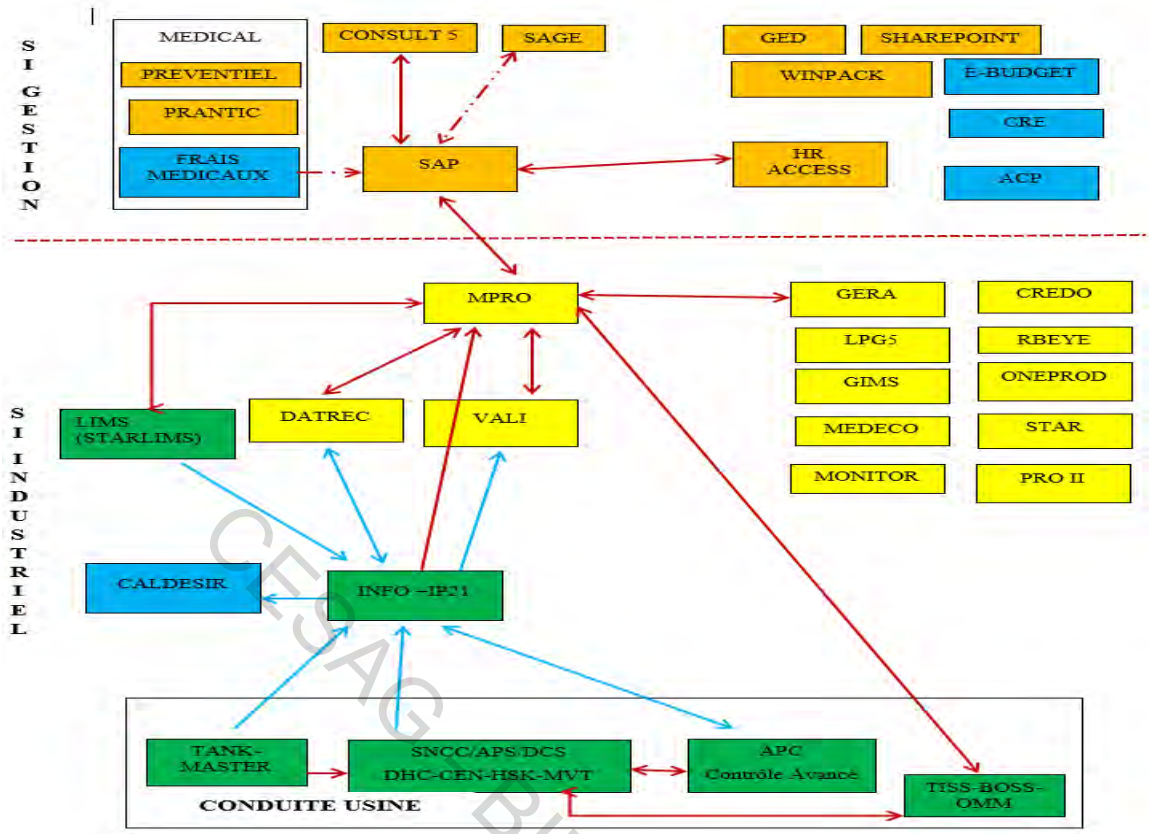
❖ **Constat**

- **Forces**

Il existe une liste d'application qui permet à la SIR de répondre à quelques besoins qui rentre en compte dans l'atteinte de ses objectifs.

Pour mieux comprendre l'interaction entre ces applications et leur mode de fonctionnement nous avons procédé à une représentation schématique (voir figure 11).

Figure 11: cartographie des applications de la SIR.(janvier 2019)



Source : structure informatique (2019)

- **Faiblesses**

- Non maitrise de certains logiciels par certains utilisateurs comme SAP.
- Absence d'innovation de projet (application)
- Au niveau des couches métiers la plupart des structures utilisent Excel pour réaliser leur tâche ce qui se fait de manière manuel et susceptible d'erreur graves. (Par exemple les avis de règlements fournisseur, la détermination de marge brute et du résultat mensuel, trimestriel et annuel, les différents reporting se font de manières manuel.)
- Pas de chef projet pour un logiciel donné (confusion entre la maitrise d'ouvrage et la maitrise d'œuvre).

❖ **Cause**

- Manque de compétence interne.

❖ **Conséquence**

- Gaspiller les ressources de l'entreprise sur des projets peu contributifs ou mal cadrés ;

4.2.2.1.4. Management des risques SI en fonction de leurs impacts <<métiers>>

❖ **Constats**

- **Forces**

- Mise en place d'un DMZ pour les échanges via la messagerie Outlook sur internet ;

- **Faiblesses**

- Inexistence de cartographie des risques ;
- Pas de développement d'analyse des risques SI incluant leurs impacts sur les « métiers » ;
- Pas de procédure de connaissance du profil de risque spécifique relatif au SI ;
- Pas de procédure de réduction de risques inhérents à l'utilisation de technologie informatique dans le support aux « métiers » ;
- Pas de culture de maitrise des risques qui mesure l'impact sur l'activité « métiers » ;
- Les décisions structurantes en matière de SI ne s'appuient pas sur une analyse de risque structurée et partagée avec les « métiers » ;

❖ **Cause**

- Pas de responsable de management des risques SI.

❖ **Conséquences**

- La non-maîtrise des risques peut avoir des impacts importants sur l'activité de l'entreprise, notamment en termes de fiabilité, d'intégrité et de confidentialité des informations financières et commerciales.
- Un dispositif de gestion des risques informatiques inadapté aux enjeux métiers ne permet pas d'appréhender les risques majeurs de l'entreprise et peut conduire à laisser des risques informatiques non couverts ou avec un dispositif de contrôle insuffisant.

4.2.2.2. Domaine support

Dans ce domaine nous nous sommes basés sur deux vecteurs critiques.

4.2.2.2.1. Alignement de la fonction informatique par rapport au processus <<métier>>

❖ **Constat**

- **Forces**

- La structure SI est associée à certains projets de développement de la SIR.

- **Faiblesses**

- Pas de capteur proche des processus « métiers » de la SIR ;
- Pas de diffusion et gestion au sein de l'organisation SI, des connaissances et compétences « métiers » ;

❖ Cause

- Manque de compétence interne

❖ Conséquence

- Inefficacité dans la collaboration entre les « métiers » et la DSI se traduisant par : un gaspillage des ressources, la lenteur du processus de décision, l'inadéquation avec les enjeux « métiers », la frustration et l'incompréhension mutuelles, la multiplication des comités de coordination et des structures d'intermédiation

4.2.2.2.2. Pilotage des services externalisé

❖ **Constat**

- **Forces**

- Facilite la réalisation de benchmarks pour la SIR avec un certain transfert de savoir-faire ;
- Les différentes responsabilités d'échecs incombent au partenaire ;
- Amélioration de la qualité des services délivrés par la structure informatique au sein de la SIR.

- **Faiblesses**

- Perte de contrôle et dépendance vis-à-vis des consultants SAP, et réseau par la société DIGITAL EQUIPEMENT CORPORATION (D.E.C) au sein de la SIR ;
- Fuite d'informations à la concurrence ;
- Surcout pour la SIR.

❖ **Cause**

- Manque de compétence interne.

❖ **Conséquences**

- Perte de contrôle et dépendance vis-à-vis de certains fournisseurs ;
- Surcoûts par rapport à ce qui avait été prévu ;
- Fuite d'informations à la concurrence et/ou non-conformités légales ;
- Risques sociaux dans l'entreprise liés à une mauvaise gestion des actions de l'externalisation.

4.2.2.3. Domaine opérationnel

Dans ce domaine quatre vecteurs ont été jugés critique pour la gouvernance de la SIR.

4.2.2.3.1. Contrôle informatique favorisant la transparence

❖ **Constat**

- **Forces**

- Au sein du réseau de la SIR, elle dispose maintenant d'un contrôleur de domaine qui permet de gérer l'ensemble des utilisateurs de la SIR, qui contrôle l'installation de logiciel sur les machines, qui contrôle les flux d'informations sur le réseau ;

- **Faiblesses**

- La non identification des attaques sur le réseau informatique de la SIR ;
- Pas de véritable séparation des taches au niveau des accès par exemple dans le système celui qui saisit une facture est le même qui vérifie et qui enregistre ;
- Pas de personnes compétentes pour la surveillance du réseau par la non maitrise du logiciel IPSWITCH.

❖ **Conséquences**

- Ne pas avoir de visibilité sur les coûts ;
- Prendre des décisions d'externalisation sans avoir en mains des éléments économiques robustes.

4.2.2.3.2. Gestion prospective des compétences informatiques

❖ **Constat**

- **Forces**

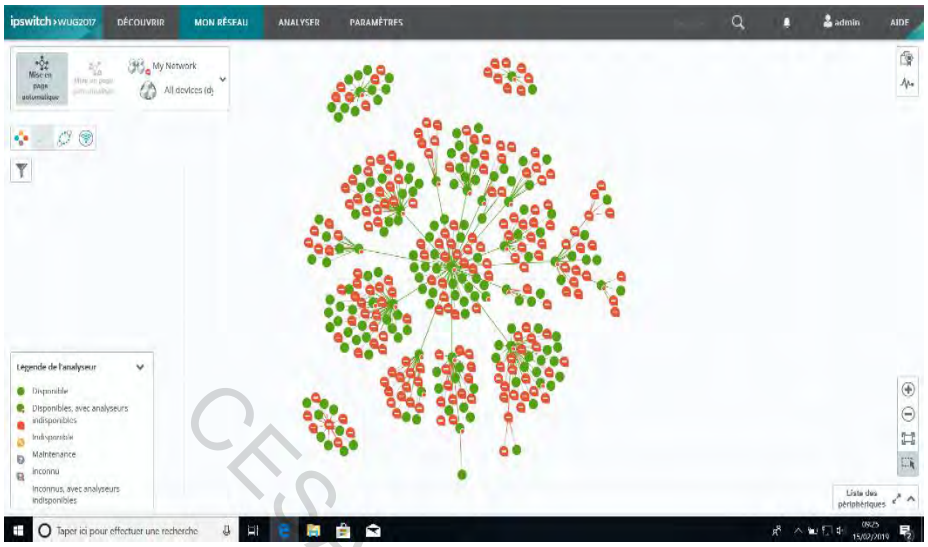
- La SIR dispose de ressources inadaptées à ses besoins ;

- **Faiblesses**

- Démotivation du personnel de la structure informatique qui ne se préoccupe pas de la maintenance de leurs compétences on constate donc une obsolescence rapide de leurs compétences ;
- Perte d'attractivité de la structure informatique qui ne parvient pas à attirer les talents nécessaires à la réalisation de nouveaux projets ;
- Vieillissement de la structure informatique ;
- Absence d'identification, de suivis d'indicateurs de performances quantitatifs et qualitatifs dans le cadre de la gestion prospective des compétences.
- La structure informatique ne correspond pas aux normes de bonne gouvernance des systèmes d'information car le profil du responsable de cette structure montre qu'il est beaucoup plus opérationnel à pouvoir maitriser le management des systèmes d'information, à penser à l'innovation de certaines applications et équipement réseau qui datent de plus d'une quarantaine d'année.
- La supervision du réseau avec le logiciel IPSWITCH a montré sur les six mois passés à la SIR que le réseau était quotidiennement instable ce qui occasionne des retards

considérables des taches critiques. La figure 12 nous montre l'indisponibilité fréquente du réseau.

Figure 12 : indisponibilité fréquente du réseau



Source : structure informatique (2019)

❖ **Conséquences**

- Avoir des ressources inadaptées aux besoins de l'entreprise et des projets à lancer ;
- Perte d'attractivité de la Structure Informatique qui ne parvient pas à attirer les talents nécessaires à la réalisation des nouveaux projets ;
- Vieillissement de la structure informatique.

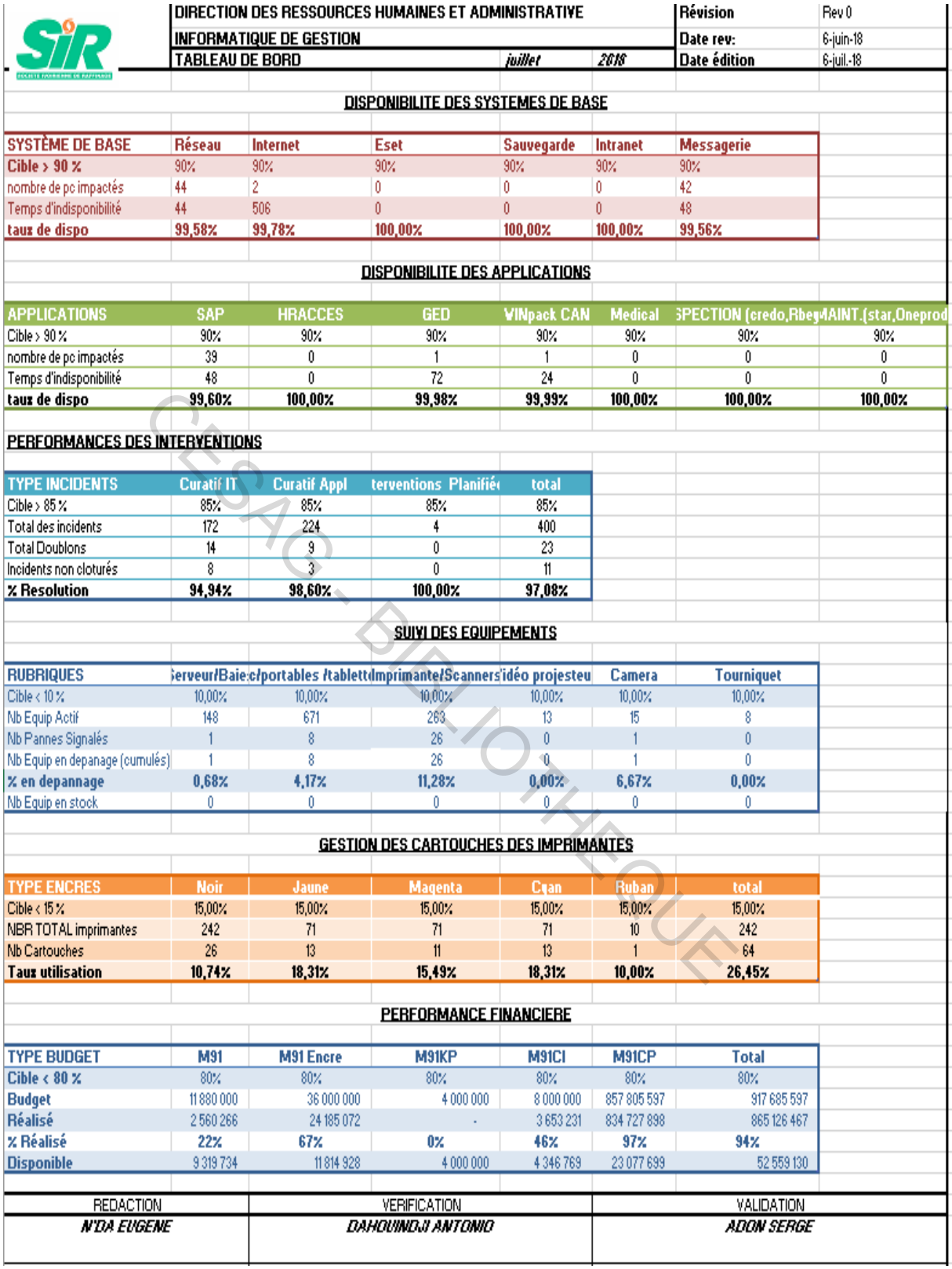
4.2.2.3.3. Gestion et mesure de la performance SI

❖ **Constat**

- **Forces**

- La structure informatique a des indicateurs permettant de mesurer sa performance en termes d'intervention par jour (nombre de cartouche changer dans les imprimantes, nombre de pannes réseau résolue par jours…) comme observé à la figure 13 :

Figure 13 : indicateur de suivi équipements, performances financières



DIRECTION DES RESSOURCES HUMAINES ET ADMINISTRATIVE				Révision	Rev 0
INFORMATIQUE DE GESTION				Date rev:	6-juin-18
TABLEAU DE BORD		juillet	2018	Date édition	6-juil.-18

DISPONIBILITE DES SYSTEMES DE BASE

SYSTÈME DE BASE	Réseau	Internet	Eset	Sauvegarde	Intranet	Messagerie
Cible > 90 %	90%	90%	90%	90%	90%	90%
nombre de pc impactés	44	2	0	0	0	42
Temps d'indisponibilité	44	506	0	0	0	48
taux de dispo	**99,58%**	**99,78%**	**100,00%**	**100,00%**	**100,00%**	**99,56%**

DISPONIBILITE DES APPLICATIONS

APPLICATIONS	SAP	HRACCES	GED	VINpack CAN	Medical	SPECTION (credo,Rbey	MAINT.(star,Oneprod
Cible > 90 %	90%	90%	90%	90%	90%	90%	90%
nombre de pc impactés	39	0	1	1	0	0	0
Temps d'indisponibilité	48	0	72	24	0	0	0
taux de dispo	**99,60%**	**100,00%**	**99,98%**	**99,99%**	**100,00%**	**100,00%**	**100,00%**

PERFORMANCES DES INTERVENTIONS

TYPE INCIDENTS	Curatif IT	Curatif Appl	terventions Planifié	total
Cible > 85 %	85%	85%	85%	85%
Total des incidents	172	224	4	400
Total Doublons	14	9	0	23
Incidents non cloturés	8	3	0	11
% Resolution	**94,94%**	**98,60%**	**100,00%**	**97,08%**

SUIVI DES EQUIPEMENTS

RUBRIQUES	erveur/Baie	portables	tablett	Imprimante	Scanners	idéo projecteu	Camera	Tourniquet
Cible < 10 %	10,00%	10,00%	10,00%		10,00%	10,00%	10,00%	10,00%
Nb Equip Actif	148	671	263		13	15	8	
Nb Pannes Signalés	1	8	26		0	1	0	
Nb Equip en depanage (cumulés)	1	8	26		0	1	0	
% en depannage	**0,68%**	**4,17%**	**11,28%**		**0,00%**	**6,67%**	**0,00%**	
Nb Equip en stock	0	0	0		0	0	0	

GESTION DES CARTOUCHES DES IMPRIMANTES

TYPE ENCRES	Noir	Jaune	Magenta	Cyan	Ruban	total
Cible < 15 %	15,00%	15,00%	15,00%	15,00%	15,00%	15,00%
NBR TOTAL imprimantes	242	71	71	71	10	242
Nb Cartouches	26	13	11	13	1	64
Taux utilisation	**10,74%**	**18,31%**	**15,49%**	**18,31%**	**10,00%**	**26,45%**

PERFORMANCE FINANCIERE

TYPE BUDGET	M91	M91 Encre	M91KP	M91CI	M91CP	Total
Cible < 80 %	80%	80%	80%	80%	80%	80%
Budget	11 880 000	36 000 000	4 000 000	8 000 000	857 805 597	917 685 597
Réalisé	2 560 266	24 185 072	-	3 653 231	834 727 898	865 126 467
% Réalisé	22%	67%	0%	46%	97%	94%
Disponible	9 319 734	11 814 928	4 000 000	4 346 769	23 077 699	52 559 130

REDACTION	VERIFICATION	VALIDATION
N'DA EUGENE	*DAHOUINOJI ANTONIO*	*ADON SERGE*

Source : structure informatique (2019)

- **Faiblesses**

- La structure informatique ne sait pas mesurer le capital immatériel de la SIR.

❖ **Conséquences**

- Absence de connaissance/manque de transparence ;
- Mauvaises décisions.

4.2.2.3.4 Gestion de la communication

❖ **Constat**

- **Forces**

- La SIR dispose d'une messagerie Outlook qui permet à ses employés de communiquer de manière journalière ;

- **Faiblesses**

- Aucune visibilité sur les succès de la structure informatique ;
- Absence de sens et de perspective vis-à-vis des directions « métiers » ;
- Manque de communication sur les risques en termes de SI.
- Indisponibilité régulière de la messagerie.

❖ **Conséquences**

- Perception de la Structure Informatique à travers les seuls incidents du SI ;
- Absence de sens et de perspective vis-à-vis de la direction générale, des directions « métiers » et des collaborateurs de la DSI.

4.3. Analyse des résultats d'audit et recommandation

Cette partie de notre travail nous permet de répondre exactement aux différentes questions que nous nous sommes posés plus haut et finalement proposer des recommandations.

4.3.1. Analyse des résultats d'audit

Selon les résultats de notre mission d'audit :

- **Structuration de la structure informatique**

L'organigramme de la SIR, comme le présente la figure 5 est loin d'être conforme à celle que propose la norme Cobit 5. La non-conformité de cet organigramme par exemple de l'absence d'un responsable de sécurité, va entrainer des atteintes à la confidentialité autrement dit le risque de divulgation d'information confidentielles donc un manque de confiance entre les parties prenantes de l'entreprise. Elle peut entrainer aussi des risques matériels qui sont la destruction totale ou partielle d'un ou plusieurs composants du système d'information. Le pire

c'est la Société Ivoirienne de Raffinage sera toujours confronté au vol, sabotage de son système d'information voire au piratage informatique.

Avec ce type d'organisation, l'entreprise est loin de pouvoir porter des réflexions stratégiques en ce qui concerne la gouvernance des systèmes d'information.

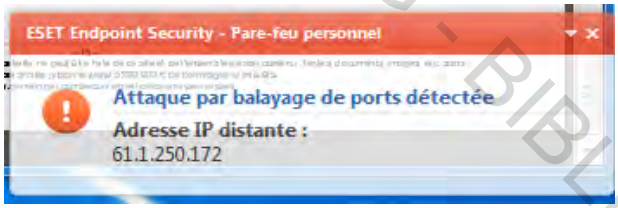
- **Communication de la structure informatique sur le risque de sécurité SI**

Les interviews montrent que la SIR a un niveau très faible sur la communication liée à la sécurité de son SI.

En effet certains agents recevaient des boites de dialogue qui leur laissait le choix de reconfigurer leur mail vers un serveur inconnu. Ne sachant quoi faire certains validaient cette reconfiguration.

De plus une information récurrente d'attaque par balayage se faisait remarquer sur certains postes de la SIR. Ce qui mettait mal à l'aise les agents face à la sécurisation de leurs données. (Voir Figure 14)

Figure 14 : menace détectée sur plusieurs machines



Source : structure informatique (2019)

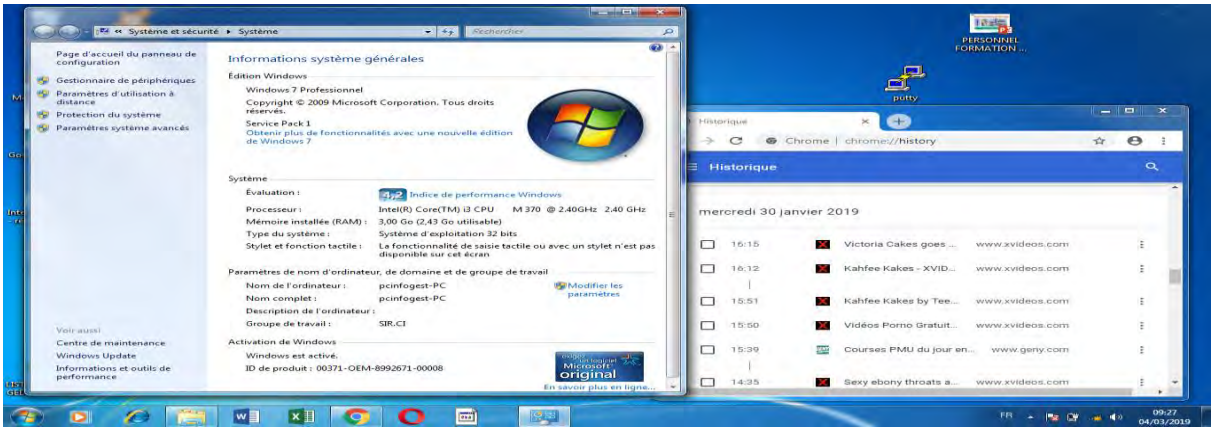
- **Politique de sécurité**

Lors de notre mission nous avons carrément constaté l'absence de politique de sécurité. Ce qui était liée au fait que chacun utilisait les outils informatiques comme bon lui semble.

De plus nous pouvons constater l'absence de la politique de sécurité par l'un des éléments très important qu'est la charte informatique.

Enfin nous voyons l'abus qui est fait du SI et son exposition au risque de sécurité par la figure 15.

Figure 15 : absence de charte informatique



Source : structure informatique (2019)

- **Nature des risques liés au SI de la SIR**

Les risques liés au SI de la SIR sont d'origines diverses. Ils sont mis à nu dans la phase de réalisation de notre audit et s'étend sur dix vecteurs.

Les risques liés au SI de la SIR sont bien réels et entravent l'atteinte des objectifs de la SIR.

- **Amélioration de la gouvernance du SI de la SIR**

Cette amélioration est clairement définie dans les recommandations et les solutions proposées.

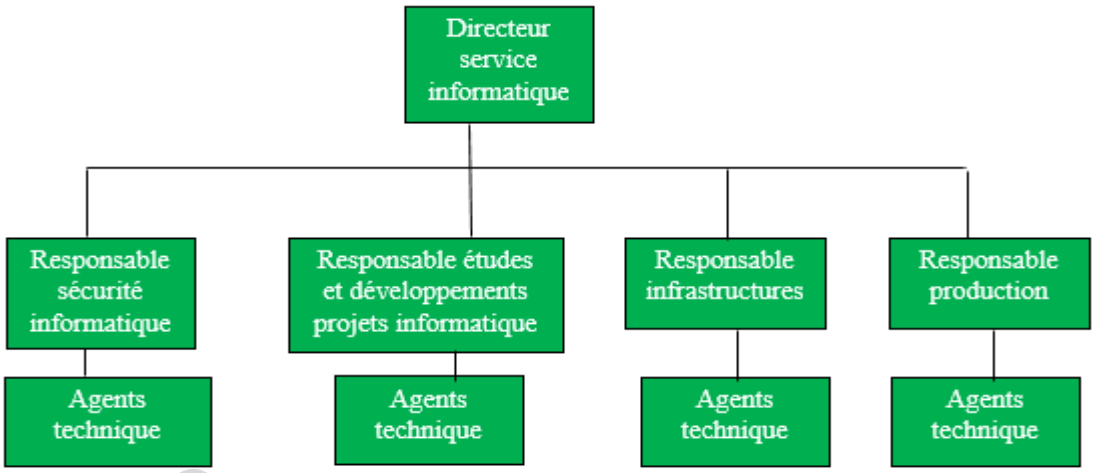
4.3.2. Recommandations

Les recommandations faites concernent plus l'amélioration de la structuration du service informatique. Car c'est l'élément par lequel la SIR pourra aligner sa stratégie a son système d'information.

4.3.2.1. Recommandations sur la structure organisationnelle

Pour être plus attractive et répondre aux objectifs stratégiques de la SIR nous proposons cet organigramme suivant : (figure 16)

Figure 16 : organigramme département informatique



Source : structure informatique (2019)

4.3.2.1.1. Rôle du directeur SI

COBIT 5 décrit le DSI comme étant « le plus haut dirigeant de l'entreprise en charge de l'alignement des stratégies IT et des stratégies d'affaires. Il est également responsable de la planification, des ressources et de la gestion de la livraison des services informatiques ainsi que des solutions pour soutenir les objectifs de l'entreprise »**.**

En d'autres termes, son rôle, en coopération avec l'ensemble des membres du Comité de Direction, consiste à participer à l'élaboration des stratégies Business et à s'assurer que les stratégies IT sont bien « embarquées » (ou alignées) avec celles de l'Entreprise. La stratégie IT devra ensuite être validée et approuvée par le Comité Stratégique qui répond au Conseil d'Administration.

COBIT 5 décrit le Comité Stratégique comme « un groupe de hauts dirigeants nommés par le conseil d'administration afin de s'assurer que ce dernier participe aux grands dossiers et décisions liés à l'IT, et qu'il en est tenu informé. Le comité est responsable de gérer les portefeuilles d'investissements en informatique, les services informatiques et les actifs informatiques en veillant à la création de valeur et que le risque soit géré. Le comité est généralement présidé par un membre du Conseil d'Administration et non par le Directeur du Système d'Information ».

Le DSI est chargé d'identifier les domaines potentiels de croissance qui auront un besoin accru du soutien informatique, et de diriger la conception et l'exécution d'une stratégie

Informatique qui construit ces fonctions essentielles dans le domaine IT. En d'autres termes, le DSI a donc comme rôle d'élaborer la stratégie IT, en alignement avec les stratégies Business en vue de satisfaire les objectifs de l'Entreprise qui eux-mêmes se déclinent de la mission qui lui a été assignée par le Conseil d'Administration. Le Comité Stratégique a, pour sa part, la charge de valider l'ensemble des stratégies et de s'assurer de leur alignement.

4.3.2.1.2. Recommandations sur les Aptitudes et compétences du DSI

Pour remplir son rôle, le DSI devra donc faire montre d'aptitudes et de compétences correspondant aux responsabilités qui lui sont assignées.

4.3.2.1.3. Alignement des stratégies du SI et des métiers de l'entreprise

- Anticiper les besoins de l'entreprise à long terme ;
- Améliorer l'efficacité et l'efficience des processus de l'organisation ;
- Déterminer le modèle de système d'information et l'architecture d'entreprise alignés avec la politique de l'Organisation et assurer un environnement sécurisé ;
- Prendre des décisions stratégiques pour la politique informatique au niveau de l'Entreprise, y compris au niveau des stratégies de sourcing ;
- Faire preuve de leadership pour la construction et la mise en œuvre de solutions innovantes sur les longs termes.

4.3.2.1.4. Gouvernance du SI

- Faire preuve de leadership concernant la stratégie de gouvernance informatique en communiquant, propageant et contrôlant les processus pertinents du département informatique entier ;
- Définir, déployer et contrôler la Management des Systèmes d'Information en ligne avec les impératifs Business ;
- Prendre en compte tous les paramètres internes et externes tels que la législation et le respect de normes de l'industrie pour optimiser les risques et le déploiement de ressources en vue de générer un bénéfice Business équilibré.

4.3.2.1.5. Gestion des relations avec les métiers

- Identifier les relations clés qui devraient être initiées pour comprendre les exigences informatiques du Business ;

- Promouvoir la vision et les opportunités que la technologie peut présenter pour l'entreprise, y compris la possibilité de transformation et son impact probable sur le Business ;
- Diriger la conception d'une procédure pratique permettant de maintenir des relations positives avec le Business.

4.3.2.1.6. Développement du business plan

- Fournir un leadership stratégique pour le développement de Business Plans pour exploiter au mieux les capacités des technologies de l'information afin de répondre aux besoins des métiers ;
- Considérer les modèles possibles et applicables de sourcing ;
- Présenter une analyse coûts/bénéfices et des arguments justifiables à l'appui de la stratégie choisie ;
- Communiquer et vendre le Business Plan aux parties prenantes de l'Enterprise en tenant compte des intérêts politiques, financiers, et organisationnels.

4.3.2.1.7. Management des risques métiers liés à l'informatique

- Diriger la définition d'une politique de gestion des risques en tenant compte de toutes les contraintes possibles, y compris les questions techniques, économiques et politiques ;
- Mettre en œuvre la gestion des risques au niveau du Système d'information grâce à l'application des politiques et procédures de gestion des risques ;
- Évaluer les risques pour le Business de l'organisation, y compris au niveau d'Internet, du Cloud et des appareils mobiles ;
- Documenter les risques potentiels et les plans de réponse.

4.3.2.1.8. Leadership et travail d'équipe

- Renforcer l'engagement sur une vision partagée afin de fournir des services client de qualité ;
- Encouragez les personnels à prendre des décisions de façon indépendante et à assumer le leadership dans leur domaine d'expertise ;
- Vaincre, grâce à sa performance, à la confiance qui lui est faite et au soutien à son leadership ;

- Créer un environnement dans lequel les membres de l'équipe sont des moteurs pour améliorer performances et la productivité ;
- Veiller à ce que les liens appropriés ou partenariats entre les équipes soient maintenues.

4.3.2.1.9. Recommandations pour une meilleure gestion financière

- Assurer la gestion financière stratégique des finances, le financement du capital ou hors trésorerie, l'amortissement des coûts de projet, la gestion d'exercice, la gestion du coût du capital.

Nous avons proposé dans ce chapitre des recommandations sur le plan stratégique, physique, organisationnel et technique afin de minimiser les risques liés à la gouvernance des SI, d'exploitation et de gestion des SI, afin de répondre aux objectifs stratégiques de la SIR et protéger les différents équipements SI pour assurer une continuité et une disponibilité complète.

4.3.2.2. Recommandations sur la gestion des risques liés à la sécurité des SI

❖ Organisation de la sécurité de l'information

L'organisation de la sécurité a pour objectif d'assurer le développement, l'implémentation et la mise à jour des politiques et des procédures de sécurité. Pour la gestion de la sécurité, il est recommandé selon la norme ISO 27002 de prendre en compte les recommandations suivantes :

- ✦ Le management de l'organisation doit avoir son implication dans la sécurité de l'information, particulièrement dans la définition de la politique de sécurité, des responsabilités, l'allocation des ressources, ...
- ✦ Etablir une revue de la sécurité de l'information en fonction des évolutions de structures ;
- ✦ Spécifier les rôles des responsables en matière de sécurité de l'information ;
- ✦ Mettre en place un système d'autorisation concernant les moyens de traitement de l'information (contrôle de l'usage d'équipements ou logiciels personnels) ;
- ✦ Assurer une veille technologique en matière de sécurité (participation à des cercles, associations, congrès,) ;

❖ Gestion des biens

- Bien que Les ressources soient répertoriées, il est important de faire une classification selon leur importance orientée suivant les 3 axes : besoin en termes de disponibilité, confidentialité et intégrité ;

- Définir les types d'actifs qui doivent être identifiés et inventoriés. Les actifs peuvent être des informations, des logiciels, des équipements matériels, des services et servitudes, des personnes ou du savoir-faire, des actifs intangibles tels que la réputation ou l'image ;
- Mettre à jour l'inventaire des types d'actifs identifiés ;
- Affecter à chaque actif identifié et inventorié un "propriétaire" qui endossera la responsabilité du développement, de la maintenance, de l'exploitation, de l'utilisation et de la sécurité de cet actif ;
- Délimiter et documenter, pour chaque actif, les règles d'usages plausibles ;
- Élaborer une procédure de revue régulière des catégorisations.

❖ Sécurité liée aux ressources humaines

- Mettre en place une procédure d'information préliminaire auprès du personnel (interne ou externe), en ce qui concernant ses devoirs et responsabilités et les exigences de sécurité de la fonction, avant tout changement d'affectation ou embauche ;
- Une note précisant les devoirs et responsabilités du personnel doit être diffusée à l'ensemble des collaborateurs de telle sorte qu'ils ne puissent nier en avoir eu connaissance ;
- Etablir une clause dans les contrats d'embauche ou dans le règlement intérieur, précisant l'obligation de respecter l'ensemble des règles de sécurité en vigueur ;
- Le personnel est tenu à respecter la politique de sécurité que la SIR va mettre en œuvre. A cet effet, une mise à niveau des employés dans le domaine de la sécurité de l'information doit être menée en planifiant des cycles de formation périodiques et en organisant des programmes de sensibilisation qui devront expliquer les méthodes de protection de l'information surtout celle qui sont critiques. Ce programme doit expliquer :
  - ✦ Les concepts de base de la sécurité ;
  - ✦ La sensibilité de l'information et le type de protection nécessaire ;
  - ✦ La responsabilité personnelle de chacun dans la gestion de la sécurité et l'application des protocoles sécuritaires ;
  - ✦ Les types de menaces (erreurs humaines, naturelles, techniques...) ;
  - ✦ Les règles et mesures générales de protection de l'information qui couvrent l'ensemble des domaines concernés (documents, micro-informatique, accès aux locaux, systèmes et applications) ;
  - ✦ Les sanctions à prendre contre le manque de responsabilité ;

- ✦ Ce programme de sensibilisation doit être réactivé régulièrement ;

- La violation de la politique sécurité et des procédures de sécurité de l'organisme par des employés devra être traitée au moyen d'un processus disciplinaire et les mesures correspondantes doivent être communiquées à tous les employés.

❖ Sécurité physique et environnementale

R.A.S.

❖ Gestion des communications et de l'exploitation

- Etablir des procédures opérationnelles d'exploitation qui doivent être documentées, maintenues à jour, rendues disponibles à toute personne en ayant besoin et approuvées par les responsables concernés ;
- Etablir, contrôler et tester formellement des mesures de sécurité pour remédier aux nouveaux risques avant mise en exploitation ;
- Définir une politique afin de lutter contre les risques d'attaque par des codes malveillants (virus, chevaux de Troie, vers) ;
- Définir une politique et des mesures de protection pour lutter contre des codes exécutables (applets, contrôle ActiveX, etc.) non autorisés (blocage ou contrôle de l'environnement dans lequel ces codes s'exécutent, authentification de l'émetteur) ;

❖ Contrôle d'accès

- Etablir une politique de gestion des droits d'accès aux zones de bureaux s'appuyant sur une analyse préalable des exigences de sécurité, basées sur les enjeux de l'activité ;
- Les droits accordés aux utilisateurs dès leur enregistrement doivent être approuvés par les propriétaires des ressources concernées ;
- Contrôler strictement le processus d'attribution (ou modification ou retrait) de droits privilégiés et d'autorisations d'accès à un individu ;

❖ Conformité

- Toutes les exigences légales, réglementaires et contractuelles doivent être définies explicitement et documentées pour le système informatique et son application par l'organisation doit figurer dans un document tenu à jour ;
- Procéder à des contrôles fréquents visant à vérifier que les logiciels installés sont conformes aux logiciels déclarés ou qu'ils possèdent une licence en règle ;
- Les opérations d'audit réalisées pour les données critiques doivent être enregistrées ;
- Passer du mode d'adressage publique au mode d'adressage privé ;
- Rédiger une charte informatique et l'appliquer le plutôt.

4.3.3. Solution proposée

La solution proposée concerne ce que peut faire dans l'immédiat les managers de la SIR afin d'aligner la stratégie des SI à l'atteinte des objectifs stratégique qu'elle s'est fixée.

❖ **Charte informatique**

Nous proposons à cet effet un document qui établira toute une rigueur sur l'utilisation des éléments du système d'information afin d'éviter certains risques de sécurité qui freinerait l'activité de la SIR.

Définition

La charte informatique (autrement appelée « charte utilisateur » ou « charte de bonne utilisation des nouvelles technologies de l'information et de la communication ») est un document destiné à régir l'utilisation des moyens informatiques mis à disposition des salariés par leur employeur dans une entreprise donnée.

Face au développement de l'usage des NTIC dans les entreprises et à la multiplication des risques inhérents (risque de voir sa responsabilité engagée pour l'employeur mais aussi risque technique lié aux virus et aux hackers), la définition de règles internes relatives à l'utilisation des nouvelles technologies s'avère aujourd'hui indispensable.

Rôle de la charte informatique

La charte informatique permet en effet d'encadrer l'usage qui en est fait par les salariés et notamment d'éviter, à tout le moins de réduire, les abus d'usage de l'Internet ainsi que les difficultés relatives à la preuve de tels abus, les salariés étant informés des règles d'utilisation et de la mise en place éventuelle de moyens de surveillance.

En outre, en interdisant ou en limitant certaines utilisations, cela contribue à assurer la sécurité du réseau informatique de l'entreprise. (Voir annexe 3)

CONCLUSION GENERALE

L'objectif de lancement de notre mission d'audit était d'évaluer le niveau de gouvernance du SI de la SIR et de dégager les déviations par rapport au référentiel Cobit 5.

A travers cet audit, nous étions en contact direct avec les responsables de la SIR et nous avons communiqué et échange avec eux pour prendre connaissance des différents éléments qui concernait notre mission. Pour réussir l'audit de la gouvernance du système d'information, nous avons travaillé avec les questionnaires relatifs à la gouvernance des SI, ce qui nous a permis de recenser les failles liées à la gouvernance des SI et les vulnérabilités du système audité.

Nous avons couvert le maximum d'aspects en nous basant sur dix vecteurs des douze qui permettent d'apprécier les risques liés à la gouvernance des SI, au cours de cette mission. Ensuite l'audit s'est concentré sur certains aspects tel que la structuration de la structure informatique.

Vu leur méthodologie de travail, nous avons constatés que les risques liés à la gouvernance des SI de la SIR étaient diverses.

Les résultats trouvés nous ont permis de faire une analyse détaillée et de répondre à la problématique de notre thème.

Notre rôle était principalement d'aider la structure à évaluer les risques de gouvernance SI et de proposer les mesures nécessaires.

Nous devons signaler que les responsables de la SIR seront les principaux joueurs et décideurs en ce qui concerne les décisions à prendre pour couvrir les risques liés à la gouvernance des SI.

Il est certain que nous avons apporté un plus à la SIR mais il faut noter que ce stage nous a permis de comprendre le monde professionnel, de travailler avec diligence, méthodes, professionnalisme et compétence. Nous avons compris les difficultés auxquelles sont confrontés les auditeurs dans l'exercice de leur mission. Dorénavant nous sommes prêts à réaliser davantage de missions pour le bénéfice des entreprises.

Les limites résident dans le fait que les bonnes pratiques peuvent limiter l'innovation. Elles peuvent devenir des freins à l'adaptation si elles ne sont pas régulièrement challengées. Elles se transforment alors en dogmes rigides.

La norme COBIT aurait-elle sa place dans une entreprise complètement robotisée ?

Bibliographie

1- OUVRAGES

1- **BECOUR (2006),** "audit opérationnel entrepreneuriat, gouvernance et performance"

2- **BERGERET, (2006)**"cartographie des risque" Edition IFACI.

3- **Cabinet d'audit, (2010)** "Compagnie Nationale des Commissaires aux Comptes",

4- **CHARREAUX G. et Wirtz** P. (2006), « *Gouvernance des entreprises : Nouvelles perspectives* », Economica.

5- **Christian DUMONT**, **(2007)** "ITIL pour un service informatique optimal" éditions EYROLLES.

6- **CAPURSO**, (2018) "audit interne et contrôle de gestion", éditions EYROLLES,

7- **Dominique MOISAND, Fabrice GARNIER DE LABAREYRE, (**2009) " COBIT pour une meilleure gouvernance des systèmes d'information", éditions EYROLLES.

8- **DUMAS, (**2003) "management et avenir », édition Vuibert.

9- **EBONDON Wa Mandzil**., **(2007),** "*Organisation et méthodologie de l'audit interne'', Audit Interne*

10- **EUSTACHE EBONDO WA MANDZILA**, **(2010),** *« Audit interne et gouvernance d'entreprise : lectures théoriques et enjeux pratiques* », Euromed- Marseille Ecole de Management.

11- **Evariste AHOUANGANSI (2018),** *Audit et Révision des Comptes*, MONDEXPERTS ABIDJAN-COTONOU-LOME.

12- **Gramling A.A., ET Myers P.M., (2006),** "*Internal Auditing's Role in ERM", Internal Auditor*, April, pp.52- 62.

13- **IFACI & institut international de l'audit social,*(2011)*** *« Des mots pour l'audit »*, imprimerie Compédit Beauregard S.A, Paris, 1995, p.26.

14- IFFACI, (2011) "gouvernance du système d'information", édition CIGREF-IFACI-AFAI, livre.

15- **IGALENS J, Peretti J M., (2008)**, "*Audit Social : Meilleures pratiques, méthodes, outils*'', Éditions d'Organisation, Paris.

16- **JACQUES renard et Sophie Nussbaumer, (2018)** "audit interne et contrôle de gestion", éditions EYROLLES.

17- **JOUFFROY, (2005)** "théorie et pratique de l'audit interne", édition d'organisation.

18- **LACOLARE Vincent (2010)**, *Pratiquer l'audit à valeur ajoutée*, éditions Afnor, Paris, 188 pages

19- **Mark salamasick, (2015)** "manuel d'audit interne améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques ", éditions EYROLLES, année,
20- **PIERRE Schick, Olivier Lemant, (2001)** "guide de self-audit" éditions d'Organisation,
21- **PHILIPE lorino, (2002)** "méthodes et pratiques de la performance", éditions d'Organisation, année
22- **RENARD J. (2010),** *Théorie et pratique de l'audit interne*, Paris, Eyrolle.
23- **RENARD Jacques**, **(2010)** « *Théorie et pratique de l'audit interne »*, 7ème édition d'Organisation, Paris, p.35.
24- **RENARD Jacques**, **(2006)** « *Théorie et pratique de l'audit interne »*, 7ème édition d'Organisation, Paris, p.49. Idem, p.51.
25- **ROBERT L., Jean-Luc A., (2007)** "Guide de la sécurité des systèmes d'information", éditions EYROLLES, livre.
26- **SEMOUD Ahmed, LAYMY Abdelhakim, (2010)**"mémoire de licence en sciences économiques Option économie des entreprises"
27- **VAURS, (2007)** "audit interne : enjeux et pratiques à l'international », éditions Eyrolles.

2- RAPPORT D'AUDIT

28- **CABINET CANADA, (2016)** "audit de la gouvernance des technologies de l'information" édité par un cabinet d'audit du canada, rapport d'audit.

3- WEBOGRAPHIE

29- https://www.formation-audit-ecofi.com/audit-gouvernance-syst%C3%A8mes-informations-si
30- https://www.formation-audit-ecofi.com/digitalisation-risques-audit-management/
31- https://www.formation-audit-ecofi.com/2017/02/21/bient%C3%B4t-nous-irons-auditer-ce-cher-watson/
32- https://fr.wikipedia.org/wiki/Syst%C3%A8me_d%27information.
33- https://www.mazars.fr/Accueil/Expertises/Conseil/Audit-des-systemes-d-information
34- https://www.journaldunet.com/solutions/expert/35634/l-audit--pratique--des-systèmes-d-information--c-est-quoi.shtml
35- https://www.cigref.fr/wp/wp-content/uploads/2019/03/2019-Guide-Audit-Gouvernance-Systeme-Information-Entreprise-Numerique-2eme-edition-Cigref-Afai-Ifaci.pdf
36- https://fr.wikipedia.org/wiki/Gouvernance_des_syst%C3%A8mes_d%27information
37- https://www.piloter.org/gouvernance/index.htm

38- https://www.piloter.org/gouvernance/pilotage-dsi.htm

39- http://www.ab-consulting.fr/blog/gouvernance/cobit-la-gouvernance-cle-du-succes-en-entreprise

ANNEXES

Annexe 1 : guide d'entretien gouvernance des systèmes d'information

Rôles et responsabilités

QUESTIONNAIRE

A. ORGANISATION ET PILOTAGE

Thème / Question	Enjeu / Risque associé	Interlocuteur cible	Réponse attendue	Phase d'audit
Un organigramme de la fonction informatique est-il formalisé et actualisé de manière régulière ?	Connaissance des parties prenantes afin d'apprécier la maîtrise de : • Rôles et responsabilités des actions et des contrôles • Séparation des tâches	DSI		
Le management de la fonction informatique est attribué à une personne dédiée ?	• Centralisation des décisions en lien avec la stratégie de l'entreprise • Mise en place de points de contrôle et de reporting par la direction	DG		
Si oui, à qui est rattachée hiérarchiquement cette personne ?	Identification du niveau de contrôle	DG		
Un responsable de la sécurité informatique est nommé au sein de l'organisation ?	Maîtrise et coordination des actions de sensibilisation et de surveillance de la sécurité de l'information	DG		
Le directeur financier a défini des points de contrôle permettant de superviser la production	Apprécier le niveau de maîtrise du système	DAF		

de l'information comptable et financière ?	d'information par le directeur financier			

B. MANAGEMENT ET RESPONSABILITÉ

Thème / Question	Enjeu / Risque associé	Interlocuteur cible	Réponse attendue	Phase d'audit
Les fiches de poste des collaborateurs en charge de la fonction informatique sont-elles formalisées ?	Maîtrise des RACI Principe de non-répudiation renforcée	DRH		
Les fiches de postes des managers Précisent-elles leur responsabilité relative au système d'information ?	Maîtrise des RACI Principe de non-répudiation renforcée	DRH		
Pour chaque application, un responsable d'application est-il nommé ?	Maîtrise du fonctionnement des applications et de leur évolution	DAF, DSI, DG, Direction métier		
Pour chaque donnée critique, un propriétaire de données est-il nommé ?	Maîtrise des inventaires, des flux et des traitements de données	DAF, DSI, DG, Direction métier		

GOUVERNANCE DES DONNÉES

QUESTIONNAIRE

Thème / Question	Enjeu / Risque associé	Interlocuteur cible	Réponse attendue
Les référentiels inclus dans le périmètre de l'audit sont-ils uniques ?	Fiabilité et intégrité des données auditées. Ex. : fiche client en doublon	Personne en charge > identifier selon la taille et l'activité de	

		l'entreprise : DSI, DAF, DG, autre…	
Qui est habilité à créer, supprimer, mettre à jour les données référentielles (création d'un nouveau fournisseur, modification d'une fiche client, etc.) ?	• Fiabilité et intégrité des données • Risque de fraude si la SOD n'est pas respectée		
Qui valide les spécifications lors d'un projet (changement de logiciel comptable par exemple) ? Comment sont formalisées ces spécifications ?	• Exhaustivité • Fiabilité Ex : reprise de données		
Cette responsabilité est-elle formalisée dans une charte ou une politique d'entreprise ?	Fiabilité des données si les rôles et responsabilités ne sont pas définis et/ou communiqués, ce qui introduit de l'ambigüité > nécessité d'un RACI	La DG doit être impliquée sur ce point, quelle que soit la taille et l'activité de l'entreprise	
Existe-t-il un registre de classification des données ?	• Exhaustivité (plan de continuité d'activité) • Conformité • Ex. : quelles données sauvegarder, archiver et restaurer en priorité ?	Responsables métiers	
Le logiciel comptable est-il hébergé en interne ou bien est-il géré par un tiers, voire dans le cloud ?	• Disponibilité des données • Conformité • Ex. : clause d'auditabilité		
Si le logiciel est géré par un tiers, les dispositions contractuelles prévoient-	• Disponibilité des données		

elles les conditions de mise à disposition des données ?	• Conformité • Ex. : clause d'auditabilité		
Ces dispositions sont-elles testées et mesurées régulièrement ?	• Disponibilité des données • Conformité • Ex. : clause d'auditabilité		
Y a-t-il un projet GDPR dans l'entreprise ?	Conformité		
Quelles sont les dispositions en matière de sécurisation des données ? Sont-elles testées et à quelle fréquence ?	• Exhaustivité • Fiabilité • Risque de fraude		

CONTRÔLE INTERNE DES SI

QUESTIONNAIRE

Thème / Question	Enjeu / Risque associé	Interlocuteur cible	Réponse attendue
Existe-t-il une matrice de définition des rôles utilisateurs dans l'entreprise ?	Séparation des fonctions	DSI	
Les autorisations d'accès font-elles l'objet de revues qualitative et quantitative ?	Analyse des comportements des utilisateurs dans le cadre de la prévention des fraudes	DSI	
Les demandes d'évolution sur le SI financier sont-elles tracées ? Si oui, comment ? Quel est le processus de validation ?	Vérification des autorisations accordées en lien avec chaque modification pour prévenir l'introduction de biais dans les applications	DSI	

Qui met en production les développements ? Suivant quelle procédure ?	Revue des rôles et responsabilités en lien avec la surveillance du respect de la séparation des fonctions	DSI	
Les procédures de sauvegarde sont-elles formalisées ? Si cloud, les clauses contractuelles sont-elles conformes aux besoins de l'entreprise (RPO, RTO) ?	Garantie de reprise et de continuité d'activité	DSI et DAF	
Des tests de restauration sont-ils menés ? Sur quel périmètre, avec quelles parties prenantes et avec quelle fréquence ?	Garantie de reprise et de continuité d'activité	DSI et DAF	

COUVERTURE ET COHERENCE DU SYSTEME D'INFORMATION

QUESTIONNAIRE

Thème / Question	Enjeu / Risque associé	Interlocuteur cible	Réponse attendue	Phase d'audit
A. Composantes du SI Le système d'information est-il basé sur un ERP ?	• Niveau d'intégration du système d'information • Nombre importants d'interface à contrôler • Exposition à la contagion des anomalies en cas de faiblesse de contrôle	Personne en charge > identifier selon la taille et l'activité de l'entreprise : DSI, DAF, DG, autre…	OUI	
A. Composantes du SI Une dépendance forte existe entre les applications, les	• Continuité d'activité et capacité d'évolution du SI	DSI et/ou DAF	OUI	

choix technologiques et les choix d'infrastructures				
A. Composantes du SI Existe-t-il des applications dites « périphériques » de type Excel ou Access ?	• Accès aux données : fichiers extra-système peu sécurisés • Intégrité : données et calculs ouverts et non protégés	DSI et/ou DAF	OUI	
B. Connaissance du SI et couverture fonctionnelle Une cartographie du système d'information est formalisée et maintenue à jour de manière régulière ?	• Connaissance des applications sources et des traitements • Maitrise des risques liés aux évolutions du SI	DSI et/ou DAF	OUI	
B. Connaissance du SI et couverture **Fonctionnelle.** Les flux ayant un impact sur l'information comptable et financière sont identifiés ?	• Connaissance des applications sources et des traitements • Maitrise des risques liés aux évolutions du SI	DSI et/ou DAF	OUI	
B. Connaissance du SI et couverture **Fonctionnelle.** Une matrice de couverture des processus par les applications est renseignée	• Connaissance des applications sources et des traitements • Maitrise des risques liés aux évolutions du SI	DSI et/ou DAF	OUI	

CONTRÔLE DES ACCÈS

QUESTIONNAIRE

Question	Enjeux / Risques associés	Interlocuteur concerné	Réponse attendue
L'organisation auditée a-t-elle documenté sa politique de contrôle d'accès et tient-elle à jour une matrice des autorisations ?	Accès non autorisés, fraudes…	DG	
Concernant la gestion des droits d'accès : - Qui décide de l'attribution / retrait des droits d'accès ? - Qui saisit la création / suppression des droits d'accès ?	Accès non autorisés, fraudes…	DG, DSI	
Une procédure formelle d'attribution /retrait des droits d'accès par utilisateur est-elle définie, avec circulation d'informations entre les services concernés ?	Accès non autorisés, fraudes…	DG, DSI, chefs de services	
L'attribution des droits d'accès se fait elle par : - Aucun accès sauf autorisations explicites Ou - Accès à tout sauf interdictions explicites	Droits d'accès trop larges Fraudes	DSI	
Les utilisateurs ont-ils l'interdiction de divulguer, communiquer, partager leur mot de passe ?	Accès non autorisés, fraudes	DG	
Les mots de passe ont-ils une obligation de complexité (longueur mini, 3 types de caractères différents…)	Accès non autorisés, fraudes	DSI	
Les postes de travail se verrouillent-ils automatiquement après quelques minutes d'inutilisation ?	Accès non autorisés, fraudes	DSI	

Tout équipement (ordinateur, tablette, smartphone), connecté au système d'information a-t-il fait l'objet d'une procédure formelle et préalable d'approbation ?	Accès non autorisés, fraudes	DSI	
Le réseau wifi est-il connecté au réseau de production ?	Accès non autorisés, vol de données, sabotage, fraude	DSI	
Les points d'accès au système d'information (serveurs, postes de travail, imprimantes, scanners…) font ils l'objet d'une sécurité physique appropriée (porte avec verrou et badge d'entrée, surveillance, caméras…) ?	Accès non autorisés, vol de données et de matériel, sabotage, fraude	DSI	
Si connexions distantes, depuis l'extérieur, existe-t-il des mesures de sécurité complémentaires, comme authentification à deux facteurs, limitation adresses IP entrantes…?	Accès non autorisés, vol de données, sabotage, fraude	DSI	
Les ressources de l'entreprise, accessibles en ligne par le public, font elles l'objet de mesures de sécurité spécifiques, régulièrement auditées ?	Accès non autorisés, vol de données, sabotage, fraude	DSI	
Les journaux de connexions sont-ils examinés : - régulièrement ? - Les échecs de connexion sont-ils analysés ?	Détection des tentatives de piratages.	DSI	
Existe-t-il une politique de chiffrement des données sensibles (mots de passe, supports nomades…) ?	Vol de données, accès non autorisé, fraude	DSI	
Dans la liste des utilisateurs du SI, les comptes d'administration ont tous les droits.	Accès non autorisé, fraude	DSI	

- Comment ces comptes sont-ils supervisés ? - Leurs actions sont-elles enregistrées et surveillées ?			
Les fonctions de développement informatique, de tests et d'exploitation sont-elles séparées, avec du personnel différent ?	Fraude	DSI	

CONDUITE DE PROJETS

QUESTIONNAIRE

Thème / Question	**Enjeu / Risque associé**	**Interlocuteur cible**	**Réponse attendue Ou éléments à collecter**	**Phase d'audit**
Quels sont les projets en cours ou prévus au cours de l'exercice fiscal ?	Implication suffisante des équipes comptabilité/finance	DSI, DAF	Liste des projets	Intérim
Ces projets ont-ils un impact sur les process et/ou les états financiers ?	Impact sur la certification des comptes	DAF	Une réponse claire et argumentée	Intérim
Pour chaque projet, une charte a-t-elle été écrite, partagée et acceptée par les parties prenantes ?	Ambiguïté sur le résultat attendu et les rôles et responsabilités des parties prenantes	Toutes les parties prenantes et en particulier DAF et DSI.	oui	Intérim
Quelle est la date cible de livraison du projet ?	Périmètre de l'audit Cut-off	DAF et DSI.	Début d'exercice ou en cours d'exercice	Intérim

Existe-t-il un RACI ? Si oui, a-t-il été formalisé et communiqué à toutes les parties prenantes ?	Ambiguïté sur le résultat attendu et les rôles et responsabilités des parties prenantes	Sponsor du projet	OUI	Intérim
Qui valide les spécifications et de quelle manière ?	Impact sur les process et/ou les états financiers (ex. : refonte de la clé comptable)	Equipe comptable DAF Equipe projet	DAF, DG ou toute personne ayant l'autorité de valiser les process cibles	Intérim
Qui valide la reprise de données et de quelle manière ?	Exhaustivité, fiabilité, intégrité des données	Equipe comptable avec responsabilité du DAF	DAF, DG	Intérim
La mise en production du nouveau logiciel comptable a-t-elle lieu au démarrage du nouvel exercice ou bien en cours d'exercice ?	Cut-off Reprise des encours en cours d'exercice	Equipe projet	Démarrage si possible	Intérim
Le DAF participe-t-il effectivement au comité de pilotage ?	Sponsor suffisant en termes de management	DAF	OUI	
Si migration vers une solution cloud, le ctt prévoit-il les clauses ad hoc (auditabilité, réversibilité, GDPR) ?	Conformité Délai d'accès aux données sur demande du CAC.	Equipe projet DAF Juridique	Oui	
Phase : cadrage Le planning est-il réaliste ?	Retard du projet. Complexité d'un démarrage en cours d'exercice.	DAF, DSI	Oui	

Phase : cadrage Un PAQ a-t-il été écrit et validé par les parties prenantes ?	Détection et communication des risques projet. Rôles et responsabilités des parties prenantes. Arbitrage. Gestion des litiges.	Equipe projet DAF DSI	Oui	
Phase : Spécifications La définition des processus est-elle conforme au besoin ?	Non-respect des règles de gestion, des procédures et des principes de séparation des fonctions. Non-conformité	Equipe projet Utilisateurs	Oui + demander l'accès aux spécifications fonctionnelles	
Phase : Paramétrage La solution est-elle utilisée dans sa version standard ? Sinon, quelle est la proportion de développements spécifiques	Non-respect des règles de gestion. Difficulté de maintenance de migration future.	DAF DSI	Proportion de customisations	
Phase : Paramétrage Combien y a-t-il d'interfaces entrantes et sortantes autour de la nouvelle solution ? Quel est le niveau d'intégration global ?	Exhaustivité et fiabilité des données : risque de déficience des mécanismes d'alimentation et de déversement des données en entrée et en sortie de la nouvelle application.	DSI Equipe projet technique	Cartographie des interfaces	
Phase : Tests • Quelle est la stratégie de tests ?	Exhaustivité Fiabilité des données	Chef de projet DSI, responsable informatique	Stratégie de tests	

• Sur quel volume de données sont-ils réalisés ? • Qui a rédigé les scénarios ?	Régression fonctionnelle		Scénarios de tests	
Phase : Reprise de données Nettoyage des données à reprendre. Trans codification des règles et référentiels comptables	Risque d'exhaustivité et d'intégrité des données reprises dans le nouveau système. Exactitude des schémas comptables, exhaustivité, auditabilité.	Equipe projet DAF/DC Equipe SI	Documentation Conservation des éléments techniques temporaires (base pivot, fichiers intermédiaires)	
Le DAF participe-t-il effectivement au comité de pilotage ?	Sponsor suffisant en termes de management.	DAF	OUI	
Phase : Recette Quelle est l'organisation de la recette en termes de : • Recetteurs • Données de recette • Remontée et traitement des anomalies (outil de ticketing) • Formalisation de l'acceptation	Fiabilité des processus	DAF, DC, responsable fonctionnel	Cahier de recette PV de réception dûment signé	
Conduite du changement	Absence de sponsor	DG	Démarche	

• Quelles sont les actions de communication et d'accompagnement ? • Quelle est la répartition de ces actions sur le planning projet ?	Implication insuffisante des utilisateurs. Echec du projet Inadéquation de la solution.			
Phase : mise en production Quelle est la politique d'archivage de l'historique ?	Risque de perte de traçabilité de l'information. Perte d'accès aux informations utiles à l'activité ou réglementairement requises.	DAF	Politique formalisée	
Phase : support post-production Quelle est l'organisation en place pour traiter les anomalies et répondre aux questions des utilisateurs pendant et après la mise en production (nb. : sujet concernant également la recette et la conduite du changement)	Sécurité de l'environnement informatique : risque de perte de maîtrise dans les processus de gestion des anomalies, des incidents, de la sécurité de l'application et de l'exploitation informatique	DSI	Description de l'organisation du support	
Documentation La documentation liée au projet est-elle suffisante en qualité et en quantité. Exemples : expression des besoins, planning, note de cadrage, spécifications (fonctionnelles et	Auditabilité du projet Conformité	DG, DAF, DSI	Accès à la documentation	

techniques), cahier de recette,…				
Amortissement Le projet fait-il l'objet d'un amortissement ?	Exactitude de la comptabilisation des coûts liés au projet (opex vs. capex). Run/build et risque de finir le projet en basculant les coûts en TMA.	DG, DAF	Détail de la comptabilisation des dépenses liées au projet	
Subventions Le projet fait-il l'objet d'un CIR ?	Correcte imputation des subventions	DG, DAF	En fonction de la réponse	

Annexe 2 : questionnaires liées à l'audit de la gouvernance SI de la SIR

Tableau 9 : questionnaires d'audit

STRUCTURE ORGANISATIONNELLE ET DE GOUVERNANCE		
Les questions nous aideront à mieux comprendre le niveau ou l'existence de la gouvernance des systèmes d'information		
QUESTION	EVALUATION/ REMARQUES	
	% personnes favorables	%personnes defav.
La fonction de DSI existe-t-elle et fait-elle partie de la direction générale ?	Non elle n'existe pas c'est juste une structure sous la direction des ressources humaine. Et qui ne fait pas partie de la direction générale.	
La structure de l'organisation et ses composantes opérationnelles sont-elles Clairement agencées de sorte que la fonction des SI puisse contribuer avec efficience Et efficacité à l'atteinte des objectifs de l'organisation ?	8.33 (2)	91.66 (22)
Des organes de décision sont-ils en place pour faciliter l'alignement des besoins de L'organisation sur les services SI et assument-ils les responsabilités et un devoir de rendre compte adéquat?	0	100
Les besoins de l'organisation et les exigences en matière de services SI sont-ils définis dans les plans stratégiques et tactiques et surveillés?	0	100
Le DSI et la direction générale se réunissent-ils de manière régulière pour discuter des progrès réalisés ?	0	100
Les rôles et responsabilités sont-ils clairement définis et communiqués et les Dirigeants de l'organisation sont-ils responsabilisés et tenus de rendre compte des résultats ?	16.66 (4)	83.33 (20)
TOTAL	**5**	**94.99**
LEADERSHIP ET SOUTIEN DE L'EXECUTIF		
Les questions suivantes nous aideront à mieux comprendre le niveau d'intégration de la gouvernance des systèmes d'information au sein de l'organisation :		
QUESTION	EVALUATION/ REMARQUES	
	% personnes favorables	%personne defav.
La direction générale a-t-elle clairement défini et communiqué les rôles et Responsabilités de la fonction SI en lien avec les objectifs stratégiques et tactiques de l'organisation ?	50	50

Les rôles et responsabilités du DSI sont-ils clairement définis et communiqués ?	33.33 (8)	66.66 (16)
L'organisation reconnaît-elle dans sa stratégie que la fonction SI contribue de Manière significative à l'atteinte des objectifs et qu'elle soutient l'organisation au quotidien?	50	50
Le DSI se réunit-il régulièrement avec la direction générale et le Conseil pour débattre des prestations SI en lien avec les plans stratégique et tactique ?	12.5 (3)	87.5 (21)
La fonction des SI dispose-t-elle du financement adéquat pour répondre aux besoins de l'organisation ?	50	50
TOTAL	**39.16**	**60.83**
PLANIFICATION STRATEGIQUE ET OPERATIONNELLE		
En posant les questions suivantes, nous pourront nous faire une idée du niveau de mise en œuvre du management de la performance stratégique par la direction générale :		
QUESTIONS	EVALUATION/ REMARQUES	
	% personnes favorables	%personne defav.
Le Conseil et la direction générale considèrent-ils que les SI font une contribution stratégique à l'organisation ?	58.33 (14)	41.6(10)
Le plan stratégique de l'organisation explique-t-il comment les SI peuvent soutenir et contribuer à la création de valeur ?	0	100
Le plan stratégique est-il soutenu par des plans opérationnels tactiques intégrant les exigences et les livrables des SI ?	25 (6)	75
Existe-il des indicateurs clés de performance (KPI) utilisés par la direction générale pour mesurer et surveiller l'efficacité de la fonction SI?	0	100
Les décisions en matière d'investissements stratégiques pour les SI s'appuient-elle Sur des analyses de rentabilité et sont-elles évaluées a posteriori pour définir si le retour sur investissement prévu s'est bien produit ?	16.66 (4)	83.33 (20)
Les retours d'expérience sont-ils pris en compte en matière d'investissements SI ?	50	50
L'organisation des SI est-elle structurée efficacement en fonction de la taille et de la composition de l'organisation ?	4.16 (1)	95.83

Le DSI et l'équipe de direction de la fonction SI sont-ils qualifiés et expérimentés ?	12.5 (3)	87.5
TOTAL	**20.84**	**79.15**
PRESTATION DE SERVICE ET SUIVI DE LA PERFORMANCE		
En posant les questions suivantes, nous pourront comprendre le niveau de fonctionnement de la gestion financière des SI :		
QUESTION	EVALUATION/ REMARQUES	
	% personnes favorables	%personne defav.
Le Conseil et la direction générale ont une compréhension précise des coûts des SI et de la manière dont ils contribuent à l'atteinte des objectifs stratégiques de l'organisation ?	87.5 (21)	12.5
Les dirigeants de l'organisation mesurent-ils la valeur et les livrables des systèmes D'information ? Si oui, comment ?	50	50
Quels sont les résultats de la comparaison des coûts liés aux SI avec des organisations similaires ?	Néant	Néant
La performance du DSI est-elle mesurée à l'aide de données financières et extra financières ?	12.5 (3)	87.5
Des dispositifs de gestion des ressources sont-ils en place ? Si oui, sont-ils évalués et suivis ?	50 tous n'est pas évalué et suivi.	50
TOTAL	**50**	**50**
ORGANISATION ET MANAGEMENT DES RISQUES SI		
En posant les questions suivantes, l'auditeur interne pourra se faire une idée précise de l'environnement de la gouvernance des SI :		
QUESTION	EVALUATION/ REMARQUES	
Dans quelle mesure les processus de l'organisation sont-ils automatisés ?	Certains processus opérationnels sont automatisés pour faciliter l'accès en temps réel des informations au niveau des unités de production.	
Quel est le degré de complexité de l'infrastructure SI et combien d'applications sont utilisées ?	La complexité se situe au niveau de la sécurité du système d'information, de la prise en compte des besoins métiers. Les applications utilisées sont au nombre de 33.	
Les données sont-elles normalisées et aisément partagées entre les applications (et au sein de l'infrastructure SI) ?	Les données de part et d'autre sont déversées dans le logiciel SAP comme on le voie à la figure 10. Mais l'exploitation la maitrise du logiciel SAP reste à désirer.	
Le matériel informatique, les logiciels, les politiques, procédures et contrôles des services sont-ils normalisés ?	0	100

Quelle est la maturité des processus de gestion des SI et des cadres de référence reconnus sont-ils utilisés (ex : COBIT, ITIL, ISO) ?	Selon les différents niveaux de maturités décrit par COBIT. La SIR se situe au niveau « initialisé cas par cas » ou les processus sont mis en œuvre au cas par cas et sans méthode.	
Comment les risques sont-ils gérés en relation avec les besoins et les exigences en matière de sécurité et de conformité de l'organisation ?	La supervision du réseau de la SIR est assurée par le logiciel IPSWITCH pour sa nom maitrise d'utilisation le système reste vulnérable.	
Quelle est l'importance stratégique des SI ?	Elle est importante car elle permet de comprendre les évolutions avenir et de s'y préparer.	
TOTAL	**0**	**100**

Source : nous même

Annexe 3 : charte informatique

REPUBLIQUE DE COTE D'IVOIRE

Guide de sécurité informatique

CHARTE INFORMATIQUE

Public Cible	Date de Publication	Date de Révision	Version
			1

1. Objet

La présente Charte a pour objet de définir les conditions d'utilisation et les règles de bon usage des actifs informatiques et moyens de communication de La SIR. Elle est établie dans le respect des lois et règlements en vigueur.

La Charte pose les fondements permettant d'assurer la sécurité et la performance du système ; de préserver la confidentialité, dans le respect des droits et libertés des utilisateurs prévus par la **Loi N°2013-450 du 19 juin 2013** sur la protection des données à caractère personnel.

2. Domaine d'application

La Charte s'applique à l'ensemble des personnes qui, quel que soit leur statut, ont accès aux moyens informatiques de La SIR.

3. Moyens informatiques

L'employé doit disposer de l'ensemble des outils et informations nécessaires à l'exécution des missions qui lui sont assignés. La SIR est tenue de les mettre à la disposition de l'employé. Ce dernier est tenu d'informer son supérieur hiérarchique en cas de manquement afin de permettre à La SIR de prendre les dispositions nécessaires pour la mise en place de ces outils de travail.

Chaque utilisateur est personnellement responsable de l'usage qu'il fait des ressources mises à sa disposition. En cas de perte ou de dégradation pour cause de négligence avérée de l'employé, la responsabilité de l'agent sera engagée et La SIR pourra prendre les mesures disciplinaires appropriées.

4. Utilisations

4.1 Finalité de l'utilisation des moyens informatiques de La SIR

L'utilisation du système informatique et des moyens de communication est limitée strictement au cadre professionnel et exclusivement aux seuls besoins de l'activité et de La SIR. Toute autre utilisation est strictement interdite, ce sont par exemple les jeux, la musique, l'utilisation des réseaux sociaux ou tout autre divertissement non professionnel (tchat, vidéos).

4.2 Autorisations particulières

Toute autre utilisation des moyens informatiques de La SIR doit être préalablement autorisée par le supérieur hiérarchique et/ou le Directeur Général.

4.3 Usage d'Internet

La structure informatique met en œuvre dans le système la politique de navigation sur Internet validée par la Direction Générale de La SIR (sites Internet autorisés pour chaque collaborateur). Le collaborateur est directement responsable du contenu des sites et messageries électroniques personnelles auxquelles il se connecte, ainsi que de l'information téléchargée par ce biais, étant donné les risques d'attaques et d'infections de virus ou toute autre déconvenue. La structure SI se réserve le droit de limiter les accès à certains sites, en fonction des politiques internes de sécurité, et en cas de dommage total ou partiel de l'information contenue dans le système d'information.

Sont strictement prohibées les utilisations contraires aux lois et règlement intérieur en vigueur et notamment celles qui ont pour objet ou pour effet, la diffusion d'idéologies politiques. Sont également prohibées, les restrictions qui sont de nature à porter atteinte aux bonnes mœurs, à la dignité, à l'honneur, ou à la vie privée des personnes.

L'utilisateur doit exercer une vigilance particulière à l'égard du contenu des échanges. Il lui est notamment interdit lors de l'utilisation des comptes et infrastructures de La SIR de :

- Visualiser, télécharger, transmettre ou conserver des contenus à caractère pornographique, diffamatoire, pédophile, raciste, xénophobe, terroriste, calomnieux, portant atteinte au respect de la personne humaine et à sa dignité, incitant la personne à commettre un délit ou un crime, contraire à l'ordre public ou aux bonnes mœurs, attentatoires à l'image de marque interne ou externe de La SIR ;
- Commettre des actes répréhensibles au regard de la loi applicable, notamment en ce qui concerne la propriété intellectuelle ;
- Participer à des jeux d'argent, entretenir des relations commerciales à titre privée ;
- Transmettre ou publier des informations non publiques ou confidentielles de La SIR, des clients, partenaires ou du personnel (sauf si autorisé par la hiérarchie et protégé par des moyens adéquats validés) ;
- Réaliser une connexion internet par des moyens autres que ceux autorisés à cet usage et mis à disposition du personnel à cet effet.

La SIR se réserve le droit de faire des contrôles sur l'historique d'utilisation qui a été fait du matériel et des sites consultés.

4.4. Confidentialité

- L'utilisation du poste de travail personnel, ou des fichiers d'un utilisateur exige l'accord formel de ce dernier ;
- Le salarié s'interdit d'emporter, sauf nécessité de service, des documents hors de l'entreprise ;
- S'il s'agit de documents comportant des informations confidentielles, il devra préalablement avoir obtenu une autorisation de son supérieur hiérarchique ;
- Le salarié s'interdit de rechercher dans les documents, bases de données ou fichiers de La SIR toutes informations dont il n'aurait pas strictement besoin pour remplir sa mission ;
- Un dossier public accessible par tous sera créé pour l'échange de fichiers communs :
- L'utilisateur est responsable de la gestion de ses informations en termes de création, modification, sauvegarde, suppression et diffusion.

5. Utilisateurs

5.1 Identification des utilisateurs

Par utilisateur, on n'entend toute personne, quel que soit son statut, qui, à titre professionnel, est autorisée à accéder aux moyens informatiques et de communication de La SIR.

Pour ceux qui doivent utiliser le système informatique et moyens de communication, un login et un mot de passe personnel (ou tout autre moyen d'identification unique) leur sont attribués.

5.2 Obligations des utilisateurs

5.2.1 Règles générales

- Les utilisateurs sont tenus de respecter la Charte de bon usage du Système informatique et des moyens de communication de La SIR ;
- Les utilisateurs doivent respecter les lois et règlements en vigueur ainsi que les règles de courtoisie et de politesse lors de l'utilisation des moyens informatiques de La SIR ;
- Les utilisateurs doivent veiller à faire accepter valablement les règles posées dans la présente Charte à toute personne à laquelle ils permettraient d'accéder au système d'information et de communication ;
- Il est interdit de fumer, manger, ou boire lors de l'utilisation desdits équipements ;

- Les utilisateurs doivent faire une utilisation non abusive des moyens informatiques auxquels ils ont accès ;
- Les utilisateurs doivent respecter les mesures de sécurité des moyens informatiques prévues dans cette présente Charte.

5.2.2 Règles de sécurité

- Tout le personnel doit traiter les mots de passe comme privés et hautement confidentiels ; L'absence de conformité avec cette politique entrainera une action disciplinaire.
- Les programmes installés sur chaque équipement seront adaptés et les équipements ne pourront disposer d'aucun programme supplémentaire sans autorisation expresse de la SI ;
- Toute information détenue dans le système d'information ainsi que les supports de sauvegarde sont la propriété de La SIR et à tout moment, le responsable des Systèmes d'Information peut y accéder ou les sauvegarder ;
- Toute infraction à la sécurité de l'information ou faiblesses identifiées, suspectées doit être reportée immédiatement par écrit au Directeur Général et au responsable du Système d'Information ;
- Tous les employés doivent savoir que les brèches de sécurité ainsi que les preuves relatives à des incidents de sécurité sont enregistrées et traitées ;
- La SI doit répondre aux incidents de sécurité conformément à leur classification et priorité ;
- L'employé est responsable de toutes les actions effectuées à partir de sa machine et en conséquence est tenue d'éteindre ou verrouiller en cas de déplacement ;
- Les employés sont responsables des opérations locales ou distantes effectuées depuis leurs comptes ou sous le couvert des dispositifs de contrôle d'accès qui leur ont été attribués ;
- La Direction RH est tenue d'aviser le responsable des Systèmes d'Information et la conformité des absences (congés, repos, maladies, etc.) afin que ces derniers puissent durant cette période verrouiller les accès dudit utilisateur ;
- La SIR doit informer son personnel que toute action effectuée dans le système d'information est enregistrée.

5.2.3 Fichiers des utilisateurs

- Les fichiers contenus dans les supports informatiques sont la propriété de La SIR.

5.2.4 Préservation des matériels

- Les utilisateurs sont tenus de respecter les matériels et logiciels mis à leur disposition. Les utilisateurs qui constatent une dégradation ou un dysfonctionnement doivent, dans les plus brefs délais, en informer la structure informatique.

5.2.5 Pénétration non autorisée dans les systèmes informatiques

- La pénétration non autorisée et le maintien dans un système informatique par un utilisateur sont interdits. Les utilisateurs ne doivent pas utiliser ou tenter d'utiliser le compte d'un tiers. Est également strictement interdite toute manœuvre qui viserait à accéder aux systèmes informatiques sous une fausse identité ou en masquant l'identité véritable de l'utilisateur.

5.2.6 Usage du courrier électronique

- L'usage du courrier électronique est limité à des fins de communications strictement professionnelles et doit constituer un outil de collaboration entre les collègues et avec les tiers clients ou partenaires dans le cadre des relations de travail ;
- Tout employé faisant un usage inapproprié du service de courrier électronique se verra attribuer une sanction administrative ;
- L'accès à toute messagerie privée est rigoureusement interdit sur les ordinateurs et les téléphones portables, tout manquement sera automatiquement sanctionné ;
- Tout message sera considéré comme document valide et formel, à partir du moment où il présente la signature électronique de l'expéditeur ainsi que le destinataire sur l'impression du message en question ;
- L'utilisateur ne doit jamais écrire un message électronique qu'il s'interdirait d'exprimer oralement ou par un autre moyen (courrier, télécopie…), les propos transmis par ce biais pouvant engager la responsabilité de leur auteur et de La SIR ;
- Il s'interdit de transmettre, retransmettre ou publier des messages contribuant à un harcèlement sexuel ou moral, menaces ou insultes et de manière générale contraire aux lois en vigueur ;

- Les messages électroniques officiels doivent obligatoirement comporter la signature de l'expéditeur ;
- L'utilisateur est tenu de respecter les niveaux de confidentialités des courriers électroniques définis.

6. Conséquences des manquements à la Charte et poursuites

6.1 Mesures et sanctions applicables par les responsables informatiques

6.1.1 Mesures d'urgence

La structure informatique peut en cas d'urgence :

- Déconnecter un utilisateur, avec ou sans préavis selon la gravité de la situation ;
- Isoler ou neutraliser provisoirement toute donnée ou fichier manifestement en contradiction avec la Charte ou qui mettrait en péril la sécurité des moyens informatiques.

Un compte rendu circonstancié sera fait et transmis au supérieur hiérarchique de l'utilisateur et au Responsable du Contrôle Interne.

6.1.2 Mesures donnant lieu à information

Sous réserve que soient informés le Responsable de la gouvernance et du Contrôle interne, et le supérieur hiérarchique, la structure informatique peut :

- Avertir un utilisateur ;
- Limiter provisoirement les accès d'un utilisateur ;
- Effacer ou isoler toute donnée ou fichier manifestement en contradiction avec la Charte ou qui mettrait en péril la sécurité des moyens informatiques.

6.1.3 Mesures soumises à autorisation

Sur ordre du Responsable de la gouvernance et du Contrôle interne et/ou du Directeur Général, le responsable des Systèmes d'Information peut :

- Retirer les codes d'accès ou autres dispositifs de contrôle d'accès et fermer les comptes d'utilisateurs spécifiés ;
- Interdire à titre définitif à un utilisateur tout accès aux moyens informatiques dont il est responsable.

6.1.4 Autres sanctions internes

Sans préjudice du pouvoir de sanction des Directeurs et Responsables de département, le Directeur Général de La SIR peut prendre toutes sanctions internes qui permettraient d'assurer le respect de la Charte et le bon fonctionnement des entités.

En particulier, des sanctions disciplinaires peuvent être prises, dans le cadre des règlements relatifs à la procédure disciplinaire.

Les sanctions internes ou disciplinaires ne sont pas exclusives de poursuites civiles ou pénales.

7. Engagements Personnels du respect de la Charte d'utilisation des systèmes informatiques et moyens de communication

Je soussigné M/Mme/Mlle _____ déclare avoir pris connaissance de la CHARTE D'UTILSATION DES SYSTEMES INFORMATIQUES ET MOYENS DE COMMUNICATION applicable à La SIR. Je m'engage à en respecter les termes en raison des fonctions qui me sont attribuées au sein de la SIR.

Fait, à _____, le _____/_____/_____

Le Salarié

Signature précédée de la mention :

« Lu et approuvé »

Table des matières