Centre Africain d'études Supérieures en Gestion

CESAG BF – CCA
BANQUE, FINANCE, COMPTABILITE, CONTROLE & AUDIT

Master Professionnel en Audit et Contrôle de Gestion (MPACG)

Promotion 6
(2011-2013)

Mémoire de fin d'études

THEME

EVALUATION DES RISQUES LIES A LA SECURITE INFORMATIQUE : CAS DE LA SONABEL

Présenté par :

Mlle. OUEDRAOGO Djamila Wendlasida

Dirigé par :

M. Alain SAWADOGO
Professeur associé au CESAG

Avril 2014

DEDICACE

Nous dédions ce travail à :

- l'Eternel notre DIEU pour tous ses bienfaits ;
- notre père pour tout son dur travail, son courage et surtout son esprit de sacrifice qui nous a permis de suivre cette formation, qu'il trouve là, le fruit de ses multiples efforts ;
- notre mère qui nous reste très chère ;
- nos frères et sœurs, que cette œuvre leur serve d'exemple ;
- tous ceux qui nous sont si chers.

REMERCIEMENTS

Nous tenons à remercier le Directeur du Centre africain d'études supérieures en gestion (CESAG) pour les deux années de formation reçues au sein de son établissement.

Nous adressons nos sincères remerciements à tout le corps professoral, pour les efforts déployés afin de nous livrer un enseignement rigoureux et de qualité, plus particulièrement à Monsieur Moussa YAZI, notre directeur d'institut.

Nous traduisons aussi nos sincères reconnaissances à Monsieur Marcel COMPAORE chef de service audit et contrôle de gestion et à tout le personnel.

Nous remercions également :

- Monsieur Alain SAWADOGO, notre directeur de mémoire ;
- Monsieur Christian Yves A. ZONGO, notre maître de stage ;
- Monsieur Moussa BERE ;
- Monsieur Seydou BARRA.

Je vous prie de trouver ici toute notre reconnaissance et notre gratitude pour vos conseils et suggestions pratiques dont nous avons bénéficiés.

Enfin, nous tenons à exprimer particulièrement notre reconnaissance à tous ceux qui d'une manière ou d'une autre, nous ont apporté une aide quelconque dans la conduite de ce travail.

LISTE DES SIGLES ET ABREVIATIONS

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

AFD : Agence Française de Développement

AOF : Afrique Occidentale Française

CCCE : Caisse Centrale de Coopération Economique

CIGREF : Club Informatique des Grandes Entreprises Françaises

CNR : Conseil National de la Révolution

COSO : Committee Of Sponsoring Organizations of the Treadway Commission

DMZ : Demilitarized Zone

DNS : Domain Name System

EPIC : Etablissement Public à Caractère Industriel et Commercial

ERP: Enterprise Resource Planing

FRAP: Feuille de Révélation et d'Analyse des Problèmes

GESCLI: Gestion Clientèle

Go: Gigaoctet

IFACI: Institut Français d'Audit et Contrôle Internes

ISO: Organisation Internationale de Normalisation

ONEA: Office National de l'Eau et de l'Assainissement

PCA : Plan de Continuité de l'Activité

QCI : Questionnaire de Contrôle Interne

RSSI : Responsable de la Sécurité des Systèmes d'Informations

SAFELEC : Société Africaine d'Electricité

SGSI : Système de Gestion de la Sécurité de l'Information

SI : Systèmes d'Informations

SIGEST : Système d'Information de Gestion

SNE : Société Nationale des Eaux

SONABEL : Société Nationale d'Electricité du Burkina

SSI : Sécurité des Systèmes d'Informations

USB: Universal Serial Bus

VLAN: Virtual Local Area Network

VOLTELEC: Société Voltaique d'Electricité

WAN: Wide Area Network

LISTE DES TABLEAUX ET FIGURES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES ANNEXES

TABLE DES MATIERES

INTRODUCTION GENERALE

L'informatique est devenue un outil incontournable de gestion, d'organisation, de production et de communication. Le réseau informatique de l'entreprise met en œuvre des données sensibles, les stocke, les partage en interne, les communique parfois à d'autres entreprises ou personnes ou les importe à partir d'autres sites. Cette ouverture vers l'extérieur conditionne des gains de productivité et de compétitivité.

Il est donc impossible de renoncer aux bénéfices de l'informatisation, d'isoler le réseau de l'extérieur, de retirer aux données leur caractère électronique et confidentiel. Les données sensibles du système d'information de l'entreprise sont donc exposées aux actes de malveillance dont la nature et la méthode d'intrusion sont sans cesse changeantes. Les prédateurs et voleurs s'attaquent aux ordinateurs surtout par le biais d'accès aux réseaux qui relient l'entreprise à l'extérieur.

La sécurité du système d'information d'une entreprise est importante pour la poursuite de ses activités. Qu'il s'agisse de la dégradation de son image de marque, du vol de ses secrets de fabrication ou de la perte de ses données clients ; une catastrophe informatique a toujours des conséquences fâcheuses pouvant aller jusqu'au dépôt de bilan. On doit réfléchir à la mise en place d'une politique de sécurité avant même la création du réseau.
L'analyse des exigences de sécurité et de contrôle permet de déterminer les fonctions de sécurité requise.

Pour ce faire, une évaluation des risques s'impose d'où notre choix sur la Société Nationale d'Electricité du Burkina (SONABEL), car elle est confrontée aux innovations technologiques qui se multiplient. Elle utilise de plus en plus d'informations sous forme numérique. Il est donc important qu'elle cherche à se protéger contre les incidents qui pourraient survenir.

Sa dépendance au système d'information (SI) entraine des risques informatiques, qui par leurs conséquences peuvent mettre en cause la pérennité de l'entreprise. L'analyse de risque permet d'identifier les dangers induits par les applications et les systèmes informatiques, d'évaluer les risques et de définir des barrières de protection qui vont réduire à des niveaux acceptables, les conséquences de l'arrivée d'événements redoutés.

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

- l'absence d'évaluation de la sécurité ;

- la non intégrité des sauvegardes et confidentialité des données ;
- l'ignorance de certains risques pouvant affecter le système informatique ;
- l'absence d'une charte de sécurité informatique ;
- l'insuffisance du contrôle interne.

Les conséquences découlant des problèmes ci-dessus peuvent être :

- la destruction ou des dommages à certains actifs informationnels ;
- une perte de confidentialité, d'intégrité et de disponibilité ;
- la perte de certaines données ;
- la non maitrise des risques liés à l'informatique ;
- la non amélioration du système d'information.

Pour pallier aux différents problèmes évoqués, certaines solutions sont proposées :

- mettre à jour constamment l'état du parc informatique aussi bien matériel que logiciel ;
- améliorer la sécurisation des systèmes d'informations ;
- sensibiliser les acteurs en matière de sécurité ;
- procéder à une évaluation des risques informatiques.

La solution qui retient notre attention et semble répondre aux problèmes exposés est la dernière. Selon Desroches & al. (2003) le risque étant inhérent à l'activité humaine, toute la question est de savoir comment le découvrir, l'appréhender, l'anticiper, le quantifier, et ceci étant fait, prendre les décisions correspondantes, afin, non pas d'éliminer le risque vaine gageure et stérilisation garantis de l'initiative mais de le gérer (en éliminer certains, en réduire d'autres, et aussi, ne l'oublions pas en accepter quelques-uns mais en toute connaissance de cause).

Au vue de tout ce qui a été dit précédemment la question principale que ce mémoire permettrait de répondre serait : comment maitriser les risques dans le domaine de la sécurité informatique à la SONABEL?

D'où les questions spécifiques suivantes :

- quel est l'ensemble des processus de l'entreprise et en particulier de son système informatique ?
- les systèmes informatiques de l'entreprise répondent-ils efficacement aux besoins

des services métiers ?

- quelles sont les risques liés aux activités informatiques?
- existe-t-il un contrôle interne du processus informatique permettant de garantir la sécurité des systèmes ?
- quelles sont les différentes démarches d'évaluation des risques liés à la sécurité informatique ?

Dans le but d'apporter des éléments de réponses à toutes ces questions nous avons choisi comme thème « évaluation des risques liés à la sécurité informatique : cas de la SONABEL ».

L'objectif principal de notre étude est de dégager et d'évaluer les risques concernant la sécurité informatique.

Les objectifs spécifiques sont :

- vérifier les contrôles de sécurité effectués sur les actifs informationnels vitaux et importants de l'entreprise ;
- valider l'efficacité des mesures de sécurité mises en place;
- valider les processus d'alertes et de réaction aux incidents ou dysfonctionnements de sécurité ;
- s'assurer de la conformité aux lois et règlements ;
- sensibiliser la direction et les utilisateurs aux risques potentiels.

Le champ de notre étude se limitera essentiellement aux risques liés au logiciel « ORACLE ».
Cette étude présente beaucoup d'intérêts pour l'entreprise, pour le lecteur et pour nous-mêmes :

L'intérêt de cette étude pour l'entreprise est de pouvoir identifier les risques, évaluer les menaces, mesurer les impacts et aussi donner une assurance raisonnable du niveau de risque dans le domaine de la sécurité informatique.

Notre intérêt sera d'acquérir une bonne expérience professionnelle, à travers laquelle nous aurons l'occasion d'appliquer nos connaissances scientifiques et de confronter la notion théorique à la pratique.

Notre travail comportera deux grandes parties :

- la première sera consacrée à la revue de littérature et structurée en trois chapitres : le premier traitera la typologie des risques et la sécurité informatique, le deuxième abordera la démarche d'évaluation des risques et le troisième sera consacré à l'approche méthodologique qui sera appliquée dans la partie pratique ;
- la deuxième partie comportera : le quatrième chapitre qui présentera la SONABEL société dans laquelle nous avons effectué le stage. Le cinquième chapitre décrira les logiciels et les dispositifs de sécurité existants et le sixième chapitre sera réservé à l'évaluation des risques liés au logiciel Oracle et aux recommandations.

PREMIERE PARTIE : CADRE THEORIQUE DE L'ETUDE

En 2003-2004, le CIGREF (Club Informatique des Grandes Entreprises Françaises) et l'AFAI (Association Française de l'Audit et du conseil Informatique), qui en avaient déjà perçu l'importance, soulignaient qu'un déploiement réussi pouvait apporter une meilleure prise de décision concernant l'ensemble du système d'information afin d'accroître son efficacité, une clarification et une meilleure définition des rôles des différents acteurs, ainsi qu'une bonne connaissance des processus clés liés au SI.

Selon wikipédia, la sécurité des systèmes d'information (SSI) est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaire et mis en place pour conserver, rétablir, et garantir la sécurité du système d'information. Assurer la sécurité du système d'information est une activité du management du système d'information.

Les directions des organisations prospères qui comprennent que l'informatique doit être gérée comme une entreprise (selon les principes de bonne gouvernance), agissent pour:

- aligner la stratégie informatique avec la stratégie de l'entreprise ;
- mesurer la performance de l'informatique ;
- démontrer la valeur des investissements technologiques ;
- identifier les coûts des projets et des services informatiques ;
- gérer les ressources humaines et financières ;
- maîtriser les risques opérationnels ;
- améliorer les capacités informatiques à budget constant.

Cette première partie comprend :

- Chapitre 1 : Notion de risque et sécurité informatique ;
- Chapitre 2 : Démarche d'évaluation des risques ;
- Chapitre 3 : Méthodologie de la recherche.

CHAPITRE 1 : SECURITE INFORMATIQUE ET NOTION DE RISQUE

Le risque constitue dans le domaine économique et social, une préoccupation dont l'importance ne cesse de croître. La concentration, la dimension, la technologie et l'interdépendance des activités accroissent par leur développement l'ampleur des perturbations. Ces risques qui sont soit internes, soit externes peuvent mettre en cause la survie de l'entreprise, sa compétitivité au sein du secteur économique, sa situation financière, son image de marque, la qualité de ses produits, de son service et de son personnel (Coopers et Lybrand, 2004 :49).

Nous allons dans ce chapitre définir la sécurité informatique et relever les différents types de risque.

1.1 Sécurité informatique

1.1.1 Définition du système d'informations

Selon COSO2 (2005), un système d'information est un ensemble de moyens techniques, administratifs, et humains qui servent à la collecte, au classement et à la transmission d'informations entre les membres d'une organisation (institution, entreprise, association,..)

Nous pouvons définir aussi le système d'informations comme un ensemble de composantes interreliées qui recueillent de l'information, la traitent, la stockent et la diffusent afin d'aider à la prise de décision et au contrôle dans l'organisation.

1.1.2 Définition du système informatique

Selon Volle (2004 :21), un système informatique est un ensemble organisé de ressources (matériel, logiciel, personnel, données, procédures…) permettant d'acquérir, de stocker, de communiquer des informations sous forme de données, textes, images, sons… dans des organisations.

Selon Dayan & al. (2004 ; 1075), « Le système informatique est le support technique du système d'information de l'entreprise. Cela regroupe les moyens informatiques (serveurs et postes utilisateurs) et les moyens de communication ».

1.1.3 Enjeux de la sécurité des systèmes d'informations

Selon François PILLOU (2006), le système d'information représente un patrimoine essentiel de l'organisation qu'il convient de protéger et la sécurité informatique consiste à garantir que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu.

Plusieurs types d'enjeux doivent être maitrisés :

- l'intégrité : les données doivent être celles que l'on s'attend à ce qu'elles soient, et ne doivent pas être altérées de façon fortuite ou volontaire ;
- la confidentialité : seules les personnes autorisées ont accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché ;
- la disponibilité : le système doit fonctionner sans faille durant les plages d'utilisation prévues, garantir l'accès aux services et ressources installées avec le temps de réponse attendu ;
- la non-répudiation et l'imputation : aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées, et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur ;
- l'authentification : l'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.

Tableau 1 : Risques pour l'organisation

Domaines	Exemples de question de la part		Problèmes potentiels
	de l'utilisateur externe	du fournisseur de services et d'informations	
Authentification : détermination de l'identité de l'interlocuteur	Le serveur est-il réellement celui qu'il dit être?	L'utilisateur est-il bien celui qu'il prétend être?	Usurpation d'identité
Intégrité l'assurance que l'information stockée ou transmise n'est pas altérée	L'information reçue est-elle identique à celle émise? Mes fichiers sont-ils corrompus? L'information est-elle fiable?		Modification accidentelle ou intentionnelle de l'information hébergée ou des transactions électroniques
Confidentialité la connaissance de l'information par un groupe restreint de personnes ou de systèmes	L'information n'est-elle connue que de l'émetteur et du récepteur? L'information stockée est-elle accessible uniquement aux personnes autorisées?		Détournement de l'information, appropriation non autorisée d'informations
Autorisation la permission de faire ou d'accéder à quelque chose	Qui peut accéder à mon ordinateur pendant mon absence?	L'utilisateur distant accède-t-il uniquement aux services et informations pour lesquels il a obtenu une autorisation?	Accès non autorisé à des ressources ou informations
Non répudiation protection contre la négation d'une action accomplie	Le fournisseur de services peut-il faussement prétendre qu'il n'a pas reçu ou effectué la transaction?	L'utilisateur peut-il faussement prétendre qu'il n'a pas effectué une transaction?	Nier avoir passé une commande électronique ou avoir effectué un achat
Traçabilité garder un historique des événements	Qui a fait quoi, utilisé quoi et quand?		Impossibilité de reconstituer les étapes qui ont conduit à un incident

Domaines	Exemples de question de la part		Problèmes potentiels
	de l'utilisateur externe	du fournisseur de services et d'informations	
Intrusion accès non autorisé	Comment protéger mon système personnel?	Comment détecter les intrus? Comment protéger le serveur?	Accès non autorisés et actions malveillantes (introduction de virus ou de mouchards, modification de contenu, blocage des accès, etc.), accès non souhaités (spams)
Protection physique protection contre les accidents ou sabotage	Garder l'intégrité des informations en cas de panne de courant, dégâts des eaux, incendie, etc.		Interruption non prévue de l'opérationnel et impossibilité de redémarrage rapide, dégâts irréversibles du matériel, de données
Gestion des procédures, des ressources humaines et machines		Que doit-on faire? Qui fait quoi, qui est responsable de quoi, qui met à jour quoi? Qui peut entrer en salle machine?	Pas de contrôle, manque de rigueur dans la gestion des mots de passe, des mises à jour des fichiers d'autorisation d'accès, des fichiers d'audit, de la configuration des routeurs et firewalls, etc.

Source : Nous-mêmes, inspiré du séminaire CESAG IIA-SN (2013 :21-23)

1.1.3.1 Contexte de la sécurité des systèmes d'informations

Selon la norme ISO 17799 (2005), la sécurité de l'information est l'état de protection face aux risques identifiés et résultant de l'ensemble des mesures de sécurité prises par l'entreprise.

La sécurité de l'information englobe l'ensemble des :

- sous systèmes d'exploitation;
- réseaux de télécommunication;
- logiciels;
- applications;
- documents;
- de même que la sécurité physique des lieux et des équipements ;
- ainsi que la sécurité logique des applications et des données.

1.1.3.2 Principes de la sécurité

Pour mettre en place de bonnes pratiques de gestion de l'information et implanter une politique de sécurité de l'information, les normes ISO 17799:2005 et ISO 27001:2005 peuvent servir de guide et de référence. La norme ISO 17799:2005 indique quoi protéger et la norme ISO 27001:2005 indique comment assurer la sécurité de l'information.

Pour réduire les risques, il faut, définir ses objectifs de sécurité. Ceux-ci consistent à

- identifier les menaces ;
- déterminer les vulnérabilités et procéder à l'analyse des risques identifiés en tenant compte des paramètres suivants :
    - la sensibilité des actifs informationnels de l'entreprise ;
    - la probabilité de leur survenance ;
    - le coût des mesures proposées.

Le risque en termes de sécurité est généralement caractérisé par l'équation suivante :

RISQUE = (Menace x Vulnérabilité) / Contre mesure

L'analyse des menaces (destruction de fichiers, inondation, erreur d'acheminement, virus, incendie, etc.) permet d'en faire une liste exhaustive et de déterminer les vulnérabilités qu'elles pourraient exploiter.

Il faut procéder à l'analyse des vulnérabilités afin de vérifier si les actifs informationnels critiques (applications, infrastructure technologique, réseaux, etc.) ont été protégés adéquatement.

On entend par vulnérabilité toute faiblesse des actifs informationnels qui peut être exploitée par des menaces :

- manque de contrôle de l'accès aux locaux ;
- mauvaise gestion des supports de sauvegarde ;
- complexité des règles d'accès sur les coupe-feux et les routeurs ;
- manque d'information des utilisateurs sur les procédures de sécurité, mots de passe inadéquats, etc.

L'impact est la conséquence d'une menace, causée soit de façon délibérée, soit accidentellement, qui porte atteinte aux actifs informationnels. Les conséquences peuvent être

la destruction ou des dommages à certains actifs informationnels et une perte de confidentialité, d'intégrité et de disponibilité.

Le risque indique la probabilité qu'une menace donnée exploite des vulnérabilités et cause des pertes ou dommages à un ou des actifs informationnels de l'entreprise et affecte ses activités quotidiennes.

Une seule ou plusieurs menaces peuvent exploiter une seule ou plusieurs vulnérabilités.

1.1.3.3 Modèle pour comprendre la sécurité

Le modèle suggéré par la norme ISO 17799 utilise une démarche d'amélioration continue qui comprend quatre étapes récurrentes :

- Planifier **:** définir le périmètre du Système de Gestion de la Sécurité de l'Information (SGSI), bâtir la politique de la sécurité de l'information, procéder à l'évaluation des risques, préparer le plan d'action de la sécurité ;
- réaliser **:** mettre en place le plan d'action de la sécurité, sensibiliser et former le personnel ;
- vérifier **:** s'assurer que les mesures de sécurité mises en place sont efficaces en effectuant le contrôle des procédures, et en évaluant la fiabilité des données, réaliser périodiquement des audits du SGSI ;
- agir **:** mettre en place des mesures correctives et de prévention appropriées, implanter les améliorations du SGSI qui ont été identifiées.

1.1.3.4 Règle et pratique de la sécurité

Selon la norme ISO 17799, pour aider à protéger les informations et ressources d'une entreprise, douze thèmes spécifiques, basés sur la norme ISO 17799:2005, nous informent des premières procédures à mettre en place, des bonnes pratiques à adopter et des solutions initiales en sécurité de l'information à appliquer en vue de protéger l'entreprise contre les principales menaces et vulnérabilités.

1.1.4 Organiser la sécurité de l'information

1.1.4.1 Contexte de l'organisation de la sécurité de l'information

L'organisation de la sécurité de l'information consiste à:

- préciser les rôles et responsabilités des gestionnaires, utilisateurs, contractuels, fournisseurs de services et propriétaires d'actifs informationnels;
- assurer la protection des actifs;
- mettre en place des mécanismes de sécurité pour assurer la sécurisation de l'accès des tiers aux informations et ressources de l'entreprise.

L'organisation de la sécurité est une bonne pratique qui permet de clarifier les rôles et responsabilités des acteurs en sécurité de l'information au sein de l'entreprise et d'assurer la gestion des actifs.

1.1.4.2 Rôles et responsabilités dans l'organisation de la sécurité

Selon la norme ISO 17799 :2005, pour mettre en place une sécurité adéquate, il est indispensable d'implanter des règles de conduite et de partager les responsabilités entre les différents intervenants de l'entreprise.

Il faut donc définir les rôles et les responsabilités des personnes impliquées dans la sécurité des actifs informationnels.

Les responsabilités à l'égard de la sécurité des actifs informationnels de l'entreprise reposent sur :

- les gestionnaires qui en assurent la gestion ;
- les utilisateurs des actifs informationnels;
- les tiers, fournisseurs de services et contractuels.

Le dirigeant de l'entreprise a comme responsabilités de :

- désigner un responsable de la sécurité des systèmes d'information (RSSI);
- approuver la politique globale de sécurité, les orientations et les directives.

Le comité de la sécurité doit :

- recommander les orientations et les directives au dirigeant de l'entreprise;

- approuver les standards, les pratiques et le plan d'action de la sécurité de l'entreprise;
- assurer le suivi du plan d'action de sécurité.

Selon la norme ISO 17799 :2005, le responsable de la sécurité agit comme responsable désigné pour coordonner la sécurité de l'information de l'entreprise. À cet effet, il a la responsabilité de:

- élaborer et assurer le suivi et la mise à jour périodique du plan d'action;
- communiquer au personnel, aux clients et partenaires de l'entreprise les orientations de sécurité de l'information;
- veiller au respect de la politique de sécurité de l'information ainsi qu'à la protection des renseignements personnels et sensibles;
- informer périodiquement le comité de l'état d'avancement des dossiers.

Selon toujours cette norme, le propriétaire d'un actif informationnel doit :

- assurer la gestion de la sécurité de son actif informationnel ;
- autoriser et répondre de l'utilisation, par les utilisateurs, clients et partenaires, des données ou informations dont il est propriétaire ;
- veiller à ce que les mesures de sécurité appropriées soient élaborées, mises en places et appliquées ;
- participer à la sensibilisation des utilisateurs.

1.1.5 La politique de la sécurité informatique

Selon la norme ISO 17799 :2005, trois étapes définissent cette politique :

- la prévention (cloisonnement des informations, et règles de comportement des utilisateurs du système informatique) ;
- la défense (la surveillance du réseau, le plan de continuation de l'activité ou PCA) ;
- le contrôle (l'audit de sécurité, la revue informatique).

Pour y arriver, l'entreprise dispose de plusieurs outils :

- une meilleure définition des besoins ;
- une construction budgétaire guidée et sécurisée ;

- un arbitrage du portefeuille de projets, d'actifs informationnels ;
- un pilotage des projets destiné à améliorer la productivité ;
- une gestion des changements pour minimiser les risques et focaliser les ressources sur les demandes prioritaires.

1.1.6 Les acteurs de la sécurité informatique

Selon la norme ISO 17799 :2005, ils se présentent comme suit :

- les utilisateurs ;
- les informaticiens ;
- le Responsable de la sécurité des systèmes d'informations (RSSI);
- le Comité de pilotage ;
- le comité technique informatique ;
- le groupe de projet ;
- le Chef de projet utilisateur ;
- le Chef de projet informatique.

1.2 Définition du risque

Il existe plusieurs définitions du risque et nous en retiendrons quelques unes :

- selon l'IFACI (in Renard, 2009 :155), le risque est défini comme : « un ensemble d'aléas susceptibles d'avoir des conséquences négatives sur une entité et dont le contrôle interne et l'audit ont notamment pour mission d'assurer autant que peut se faire la maîtrise » ;
- selon Michel LAFITE (2003 :96), « le risque consiste dans la réalisation d'un événement redouté, aux conséquences négatives » ;
- selon le dictionnaire LAROUSSE (2010 : 839), le risque est décrit comme un danger, inconvénient plus ou moins probable auquel on est exposé ;
- selon Henry LY (2005 :125), le risque peut se définir comme un hasard que l'on court d'une perte ou d'un dommage. En d'autres termes peut être considéré comme risque, un évènement potentiel engendrant des pertes ou dommages.

A la suite de ces définitions, nous retenons que les composantes d'un risque sont la gravité ou les conséquences de l'impact ou la probabilité qu'un ou plusieurs évènements se produisent. Le risque se mesure donc en termes de conséquences et de probabilités.

1.3 Typologie des risques encourus par les entreprises

Il s'agit ici de lister les différents risques rencontrés en général. La classification peut être faite selon l'origine, l'activité, la nature et le niveau.

1.3.1 Typologie des risques selon l'origine

Selon l'origine, nous pouvons citer :

- le risque interne : c'est le risque lié à l'organisation de l'entreprise, son management, ses processus, ses systèmes d'informations et ses facteurs sont en grande partie maîtrisables ;
- le risque externe : c'est le risque lié à l'environnement de l'organisation, son activité, son marché, ses concurrents et ses facteurs sont difficilement maîtrisables ;
- le risque de pilotage : c'est le risque lié aux informations nécessaires pour prendre les bonnes décisions (reporting financier, tableaux de bord…).

1.3.2 Typologie des risques selon l'activité

Selon l'activité nous avons :

- le risque économique et financier : il englobe les risques qui menacent les flux liés au titre financier et relèvent du monde économique ou réel (risques politiques, naturels, d'inflation et d'escroquerie...) ;
- le risque social : c'est l'ensemble des facteurs internes ou externes à l'entreprise d'origine humaine, sociale, économique, législative, politique, liés à la communication de l'entreprise ou des médias susceptibles d'affecter temporairement, durablement, voire définitivement le fonctionnement de l'entreprise concernée ;
- le risque environnemental : c'est l'ensemble des facteurs internes et externes liés à l'environnement dans lequel fonctionne l'entreprise et susceptibles d'empêcher l'atteinte de ses objectifs ;
- le risque opérationnel : c'est le risque de pertes qui provient des erreurs du personnel au sens large, des systèmes ou processus, ou des évènements externes.

1.3.3 Typologie des risques selon la nature

Les différents risques identifiés selon la nature sont :

- le risque inhérent : c'est le risque qu'une erreur significative se produise compte tenu des particularités de l'entreprise, de ses activités, de son environnement, de la nature des comptes et de ses opérations. Selon IFACI, PRICEWATERHOUSECOOPERS & al. (2005), le risque inhérent (ou risque brut) désigne le risque auquel l'entité est exposée en l'absence des mesures prises pour modifier la probabilité d'occurrence ou l'impact de ce risque. Le risque inhérent d'une entreprise peut aussi correspondre dans son ensemble à la probabilité selon laquelle ses résultats se développent de manière imprévisible. c'est le risque lié au secteur d'activité de l'entreprise ; ce risque ne dépend pas du dispositif de contrôle mis en place par l'entreprise ;
- le risque de non contrôle : c'est le risque que le système de contrôle interne de l'entreprise ne prévienne pas ou ne détecte pas de telles erreurs. C'est le risque lié aux insuffisances du dispositif de contrôle mis en place au sein d'une entreprise ;
- le risque de non détection : c'est le risque résiduel après le passage de l'audit interne. Ce risque est dû, soit à une mauvaise interprétation des conclusions d'une mission d'audit, soit à une insuffisance d'investigation lors des travaux d'audit ;
- le risque résiduel : c'est le risque qui subsiste après l'application des politiques de maîtrise des risques. Selon Schick (2010 :67), un risque résiduel correspond à un risque brut non couvert ou mal couvert par un dispositif de contrôle interne absent ou défaillant.

1.3.4 Typologie des risques selon le niveau

Dans cette catégorie, nous pouvons citer :

- le risque potentiel : c'est un risque commun à toutes entreprises qui est susceptible de se produire si aucun contrôle n'est exercé pour l'empêcher ou le détecter et corriger les erreurs qui pourraient en résulter. Ce risque est identifié à partir des guides professionnels et de l'expérience de l'auditeur ;
- le risque matériel : c'est un risque qui s'est déjà matérialisé dans l'entreprise et son

impact doit être évalué afin de définir une politique efficace pour sa maîtrise ;

- le risque possible : c'est le risque potentiel contre lequel une entreprise donnée ne s'est pas dotée de moyens pour le limiter ou le détecter et le corriger. Ce risque est identifié à toutes les étapes de la mission par les diligences mises en œuvre par l'auditeur.

Ces définitions nous montrent qu'il existe plusieurs types de risques et à tous les niveaux.

1.4 Typologie des risques informatiques

Un risque informatique est un évènement susceptible de compromettre l'atteinte de l'objectif du projet informatique (dérapage de son planning, de son coût) ou de l'objectif de l'activité économique (performance des systèmes, pérennité des outils, sécurité des données) (Desmoulins, 2009 :216).

Les risques informatiques peuvent être classés en trois (3) catégories à savoir : les risques humains, les risques techniques et les risques logiques.

1.4.1 Les risques humains

Les risques humains sont très importants et de plusieurs types. Ils concernent les utilisateurs au même titre que les informaticiens :

- la maladresse : dans toute activité, les humains commettent des erreurs, il leur arrive donc d'exécuter un traitement non souhaité, d'effacer involontairement des données ou des programmes ;
- l'inconscience et l'ignorance : certains utilisateurs des outils informatiques sont encore inconscients ou ignorants des risques encourus par les systèmes qu'ils utilisent et introduisent souvent des programmes malveillants sans le savoir. Des manipulations inconsidérées (autant avec des logiciels que physique) sont aussi courantes ;
- la malveillance : certains utilisateurs pour des raisons très diverses peuvent volontairement mettre en péril les systèmes d'informations en y introduisant des virus ou des mauvaises informations dans une base de données. De même il est relativement aisé pour un informaticien d'ajouter délibérément des fonctions cachées lui permettant, directement ou avec l'aide de complices, de détourner à son profit de l'information ou de l'argent ;
- le détournement de mot de passe : un administrateur système ou réseau peut modifier les mots de passe d'administration lui permettant de prendre le contrôle d'un système

ou d'un réseau ;

- l'ingénierie sociale : qui consiste à exploiter la confiance humaine pour obtenir des informations en vue de les exploiter à d'autres fins (publicitaire par exemple) qui serviront à mener des attaques ou à faire effectuer certaines actions par les victimes en se faisant passer pour quelqu'un d'autre. Elle peut se faire au moyen d'une simple communication téléphonique ;
- l'espionnage : utilise les mêmes moyens pour obtenir des informations sur des activités concurrentes, les politiques de prix, les clients, projets en cours.

1.4.2 Les risques techniques

Ce sont ceux liés aux pannes inévitables des matériels ou des systèmes :

- risques liés aux matériels : la plupart des composantes électroniques, produits en grandes séries, peuvent comporter des défauts. Ils finissent un jour ou l'autre par tomber en panne. Certaines de ces pannes sont assez difficiles à déceler car intermittentes ou rares. Parfois elles révèlent d'une erreur de conception ;
- risques liés aux logiciels : les systèmes d'exploitation et les programmes sont de plus en plus complexes car ils font de plus en plus de choses. Ils nécessitent l'effort conjoint de dizaines, de centaines, voire de milliers de programmeurs. Ces programmeurs peuvent faire des erreurs de manière individuelle ou collective que les meilleures méthodes de travail et les meilleurs outils de contrôle ou de test ne peuvent pas éliminer en totalité ;
- risques liés à l'environnement : les machines électroniques et les réseaux de communications sont sensibles aux variations de température ou d'humidité (tout particulièrement en cas d'incendie ou d'inondations) ainsi qu'aux champs électriques et magnétiques. Il est possible qu'un ordinateur tombe en panne de manière définitive ou intermittente à cause de conditions climatiques inhabituelles ou par l'influence d'installations électriques notamment industrielles.

1.4.3 Les risques logiques

Il s'agit ici des programmes malveillants et de certaines attaques utilisés par les pirates.

1.4.3.1 Les programmes malveillants (malware en anglais)

Ils peuvent être subdivisés comme suit :

- les chevaux de Troie : selon Laurent Bloch & al. (2007 :57), cette expression décrit un programme nuisible qui se présente sous un jour honnête, utile, ou agréable, et qui une fois installé sur un ordinateur y effectue des actions cachées et pernicieuses;
- les virus : un virus est un programme qui cherche à se propager via d'autres programmes en les modifiants ou en s'accrochant à ceux-ci. Chaque programme infecté contribuant à la propagation, l'infection est souvent rapide. Pour s'introduire dans les ordinateurs, un virus utilise des supports de données amovibles comme les clés USB, les réseaux, les messages électroniques ou internet ;
- les vers : contrairement aux virus, les vers ne s'attachent pas aux fichiers exécutables ils se transmettent d'un ordinateur à l'autre par des connexions réseau ou entre ordinateurs ;
- le wabbit : programme qui se réplique par lui-même mais qui n'est ni un vers, ni un virus ;
- le backdoor : toujours selon Laurent Bloch, c'est un logiciel de communication caché, installé par exemple par un virus ou par un cheval de Troie, qui donne à un agresseur extérieur accès à l'ordinateur, victime par le réseau.
- le Spyware : collecteur d'informations personnelles sur l'ordinateur d'un utilisateur sans son autorisation, et en envoyant celle-ci à un organisme tiers ;
- le keylogger : programme généralement invisible installé sur le poste d'un utilisateur et chargé d'enregistrer à son insu ses frappes clavier ;
- l'adware : collecte des informations personnelles et permet d'afficher des publicités ciblées ou de rediriger automatiquement vers des serveurs web lorsque l'utilisateur tape certains mots clés ;
- l'exploit : programme permettant d'exploiter une faille de sécurité d'un logiciel ;
- le rookit : ensemble de logiciels permettant d'obtenir les droits d'administration sur une machine, d'installer un backdoor, de truquer les informations susceptibles de

révéler la compromission et d'effacer les traces laissées par l'opérateur.

1.4.3.2 Attaques par messagerie

Ce sont entre autres :

- spam ou pourriel : il consiste en « communications électroniques massives, notamment de courrier électronique, sans sollicitation des destinataires, à des fins publicitaires ou malhonnêtes » (Laurent Bloch, 2007 :60).
- pushing ou hameçonage : technique consistant à créer une réplique presque parfaite d'un site web qui entreprend d'extorquer à des utilisateurs leurs données d'accès personnelles au moyen d'un formulaire sur le site web contrefait ;
- hoax ou cannular informatique : désigne un courrier électronique incitant le destinataire à retransmettre le message à ses contacts pour divers prétextes. Dans d'autres cas, ils incitent l'utilisateur à des manipulations dangereuses sur son poste (par exemple la suppression d'un fichier prétendument lié à un virus).

1.4.3.3 Attaque sur le réseau

Ces attaques peuvent être :

- le sniffing : technique permettant de récupérer d'une part toutes les informations transitant sur un réseau, et d'autre part les mots de passe des applications qui ne chiffrent pas leur communication, et identifier les machines qui communiquent sur le réseau ;
- le spoofing : technique consistant à prendre l'identité d'une autre personne ou d'une autre machine. Il est souvent utilisé pour récupérer des informations sensibles, que l'on ne pourrait pas avoir autrement ;
- le deni de service : technique consistant à générer des arrêts de service, et empêcher le bon fonctionnement d'un système.

Conclusion :

Aujourd'hui, l'hypothèse réaliste demeure que la sécurité ne peut être garantie à 100 % et requiert le plus souvent la mobilisation d'une panoplie de mesures y compris celle des « leurres » reposant sur l'idée qu'interdire ou en tout cas protéger l'accès à une donnée peut consister à fournir volontairement une information « calibrée et visible » servant de paravent à l'information sensible…

CHAPITRE 2 - DEMARCHE D'EVALUATION DES RISQUES

Le risque est un concept selon lequel l'entreprise exprime ses inquiétudes concernant les effets probables d'un événement sur les objectifs de l'entité dans un environnement incertain. Dans la mesure où il est imprévisible, l'entreprise doit tenir compte d'une gamme d'événements possibles qui pourraient intervenir dans un univers incertain. Chacun de ces événements pourrait avoir une conséquence significative sur l'entité et sur ses objectifs : les effets négatifs sont qualifiés de « risques » et les effets positifs d' « opportunités ».
Par conséquent, l'évaluation et la gestion des risques par l'entreprise sont les deux outils modernes de planification de la gestion. Le lien entre l'audit et la gestion des risques se trouve dans l'évaluation des risques et de ses conséquences sur la réalisation des objectifs définis.

2.1 Définition et objectifs de l'évaluation des risques

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

2.1.1 Définition de l'évaluation des risques

L'évaluation des risques est la première étape dans un processus de management des risques, pour les entreprises dépourvu d'une culture de risk management. Selon les normes de fonctionnement et normes de mise en œuvre associées, l'évaluation des risques doit être au moins annuelle et prendre tous points de vue de l'entreprise, et cette évaluation s'exprime sous la forme d'une cartographie des risques.
L'évaluation des risques est donc le processus qui commence par une inspection approfondie de l'entreprise en vue d'identifier entre autres les éléments, situations et procédés qui peuvent causer un préjudice. Une fois cette étape terminée, il faut évaluer la probabilité et la gravité du risque, puis déterminer quelles mesures adopter afin d'empêcher le préjudice de se concrétiser.

Ajoutons à cela un autre point de vue selon lequel l'évaluation des risques consiste à l'identification et à l'analyse des facteurs susceptibles d'affecter la réalisation des objectifs. Il s'agit d'un processus qui permet de déterminer comment ces risques devraient être gérés. L'évaluation des risques à travers la cartographie des risques est donc un outil de gestion des risques, de gestion des ressources et de communication.

2.1.2 Objectifs de l'évaluation des risques

L'évaluation des risques doit conduire à identifier les actions à mener en priorité pour maîtriser autant que faire se peut, les risques auxquels on est exposé (Barthelemy & al, 2004 :173). Le processus d'évaluation des risques a pour objectif l'élimination d'un danger ou la réduction du niveau de risque en instaurant des mesures de maîtrise ou en adoptant des précautions appropriées, s'il y a lieu.

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

- Inventorier, évaluer et classer les risques de l'organisation ;
- informer les dirigeants pour une meilleure adaptation des activités au management des risques ;
- élaborer une politique des risques par la direction générale avec l'aide du risk manager.

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

2.2 Technique d'évaluation des risques

2.2.1 Identification des risques

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

Plusieurs techniques d'identification ont été élaborées par différents auteurs. D'après Renard (2004 :76), les techniques d'identification des risques utilisées sont :

- identification par découpage de l'activité en tache élémentaires : il s'agit d'identifier et lister toutes les tâches élémentaires de l'activité si possible de façon séquentielle. Le découpage permet de connaitre les risques que l'entreprise encourt si l'une des tâches n'est pas exécutée ou est mal exécutée. Selon Renard (2005), c'est la méthode que l'auditeur utilise pour construire son questionnaire de contrôle interne ;
- identification prenant en compte l'atteinte des objectifs : elle débute par une identification claire et précise des objectifs de l'entreprise, ensuite à chaque objectif sera affectée la menace qui lui correspond selon Alexandre (2005 :3). Cette technique est assez complexe dans sa réalisation ;
- identification basée sur les check- lists : utilisation d'une liste préétablie et exhaustive des risques. Cette liste est fonction des activités de l'entreprise et elle prend en compte tous les risques relatifs aux différentes activités de celle-ci. Cependant, l'entreprise doit veiller à une mise à jour permanente de cette liste pour éviter qu'elle ne devienne obsolète ;
- identification basée sur l'analyse historique : c'est une technique préconisée par Barroin et Ben Salem (2002 :27) et qui consiste à partir des risques déjà survenus dans l'entreprise dans le passé, d'en tenir compte dans l'identification des risques ;
- exposure analysis : elle consiste à identifier les risques qui ont un impact sur les actifs de l'entreprise. Les managers, pour atteindre leurs objectifs, utilisent les actifs de l'entreprise et doivent de ce fait se concentrer sur les risques qui touchent à ses actifs. Ces actifs peuvent être les moyens financiers, matériels, humains, immatériels. Cette techniques prend en compte la taille et le type des actifs ;
- environnemental analysis : elle consiste en une identification des risques liés aux activités de l'entreprise ;
- threat scénarios : une identification des risques basée sur les fraudes et anomalie.

Plusieurs de ces techniques peuvent être combinées pour une identification exhaustive des risques. Une fois les risques identifiés, il faut les évaluer.

2.2.2 Evaluation des risques

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

De plus, selon Curaba & al (2009 :133), l'évaluation des risques ne constitue pas une fin en soi. Elle trouve sa raison d'être dans les actions de prévention qu'elle va susciter. Sa finalité n'est donc nullement de justifier l'existence du risque, quel qu'il soit, mais, bien au contraire, de mettre en œuvre des mesures effectives, visant à l'élimination des risques conformément aux principes généraux de prévention.

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

L'évaluation des risques est une étape centrale du management des risques. Le résultat de ce travail déterminera les grandes orientations du management des risques (stratégie, politique, etc.) et constituera le socle du travail de restitution sur les risques (matrice de criticité) de l'entreprise. Les principes sont :

- l'évaluation est individuelle. Il est souhaitable que les données d'évaluation soient le produit d'une analyse personnelle ;
- l'évaluation des risques n'est pas un travail de notation ou d'appréciation des différents responsables fonctionnels ou de processus. Il faut nécessairement veiller à ce que ce travail soit le plus objectif possible ;
- l'appréciation de la probabilité est une estimation très fine des facteurs qui rendent favorable l'apparition du risque. Il peut s'agir de facteurs internes ou externes ;
- l'appréciation de la gravité est une estimation très fine des impacts supposés de la survenance du risque sur la réalisation des objectifs de l'organisation.

Il convient de ne pas surestimer des risques dont les impacts sur les objectifs stratégiques ne seraient que « locaux ». De même, il faut veiller à ne pas sous estimer des risques.

Il est important que chaque évaluateur veille à ne pas tomber dans le piège du « biais cognitif » c'est-à-dire la tendance à commettre des « erreurs » d'évaluation compte tenu de facteurs subjectifs, secondaires ou erronés.

Tableau 2 : Exemple d'échelle d'évaluation

Echelle d'évaluation selon la gravité

Niveau	Conséquences
1	Insignifiant
2	Mineur
3	Modéré
4	Majeur
5	Catastrophique

Echelle d'évaluation selon la probabilité

Niveau	Probabilité de survenue
1	Très faible
2	Faible
3	Modérée
4	Elevée
5	Très élevée

Source: Nous-mêmes, inspiré de Landwell éditions d'organisation (2005:338)

2.2.4 Hiérarchisation des risques

La hiérarchisation des risques se fait principalement suivant un ordre de criticité décroissante. Pour rappel, la criticité (C) est le produit de la probabilité d'occurrence ou de fréquence (f) du risque et de la gravité (G) des conséquences du même risque (ou impact).

C = f * G (Barthelemy & al. 2004 :11)

Elle suit les différents niveaux de déclinaison recommandés par le COSO :

- filiales;
- business unit;
- processus métiers;
- projets.

En plus de la déclinaison suggérée par le COSO, il est loisible à chacun d'orienter son analyse vers des niveaux d'analyses supplémentaires suivants :

- les fonctions (direction, département, service, etc.) suivant le niveau de finesse souhaité;
- la géographie;
- le thème de risque;

La hiérarchisation des risques obéit à une logique de priorisation afin de s'assurer que l'organisation consacre prioritairement ses ressources aux risques les plus compromettants pour la réalisation de ses objectifs.
Elle sert principalement de base de travail pour l'élaboration du plan d'audit au sein de l'entreprise.

2.2.5 Traitement et financement des risques

Selon le COSO (2005), le management des risques d'un projet repose non seulement sur son identification et sur son évaluation, mais également sur sa prise en compte. En effet, il ne suffit pas de balayer l'ensemble des risques encourus (ou qui pourraient être encourus), de les estimer et de les hiérarchiser. Il faut également les maîtriser, c'est-à-dire définir et mettre en œuvre les dispositions appropriées pour les rendre acceptables. Cela nécessite donc de définir des réponses types et de mettre en œuvre, risque par risque, un certain nombre d'actions visant soit à supprimer ses causes, soit à transférer ou partager sa responsabilité ou le coût du dommage à un tiers, soit à réduire sa criticité (en diminuant sa probabilité d'occurrence ou en limitant la gravité de ses conséquences), soit à accepter le risque tout en le surveillant
L'objectif de l'étape de maîtrise n'est pas de supprimer tous les risques potentiels afférents à l'activité de l'organisation, ce qui semble totalement illusoire, puisqu'il existera toujours des

évènements imprévisibles ou non prévu qui échapperont au contrôle des acteurs et qui contribueront au succès ou à l'échec de l'organisation ou du projet. L'objectif est plutôt de savoir comment il est possible de mieux maîtriser les risques majeurs associés au projet pour les ramener à un niveau acceptable et les rendre ainsi plus supportables.

En effet, d'après Renard (2010 :161), ces différentes actions possibles pour le traitement des risques sont:

- l'acceptation du risque : l'entreprise accepte de courir le risque. Ce choix est opportun s'il correspond à la stratégie et aux limites de tolérance définies par celle-ci, et catastrophique s'il n'est que le résultat du hasard ou de manque d'information ;
- le partage du risque : l'entreprise lie des alliances pour partager un risque entre divers acteurs de la chaine de valeur. Partager le risque, c'est aussi le réduire en souscrivant une assurance ou en mettant au point une joint venture avec un tiers ce qui revient à transférer le risque à un tiers ;
- l'évitement du risque : cessation de l'activité à l'origine du risque ;
- la réduction des risques : prendre des mesures nécessaires pour agir à la fois sur la probabilité et la gravité.

2.2.6 Suivi et contrôle des risques

Selon le COSO (2005), au fur et à mesure que le projet se déroule, le portefeuille des risques potentiels doit être réajusté en fonction des nouvelles informations recueillies.
Certains risques pouvant disparaître, d'autres apparaître ou d'autres encore, considérés initialement comme faibles, pouvant devenir rapidement inacceptables pour l'entreprise dès lors qu'ils n'ont pas été maîtrisés, le niveau d'exposition aux risques de l'organisation ou du projet est amené à changer. C'est pourquoi il est important de procéder périodiquement au suivi et au contrôle des risques encourus. L'objet de cette étape est de mettre à jour la liste des risques identifiés (par la quête d'information complémentaire), d'affiner les données caractéristiques des risques déjà connus (en particulier leur probabilité et leurs conséquences potentielles), de réévaluer leur criticité, de contrôler l'application des actions de maîtrise, d'apprécier l'efficacité des actions engagées, et de surveiller le déclenchement des évènements redoutés et de leurs conséquences.

2.2.7 La capitalisation et la documentation des risques

Selon le COSO (2005), le management des risques nécessite enfin de capitaliser le savoir-faire et les expériences acquises et d'établir une documentation rigoureuse sur les risques associés à l'organisation. Même si la plupart des évènements dommageables ne se reproduisent jamais à l'identique, il n'en demeure pas moins que l'accumulation de connaissances et les retours d'expériences doivent permettre d'enrichir la connaissance des risques potentiels et dommageables, d'accroître la réactivité à chaque niveau d'intervention, de faciliter la prise de décision et d'améliorer l'efficacité des actions de maîtrise.

Conclusion :

L'objectif à atteindre aujourd'hui est celui d'un système informatique aligné sur les objectifs métiers créant de la valeur ajoutée.

Dès lors, les sociétés doivent considérer l'importance d'une bonne gouvernance informatique qui, loin de toute vision endogène, n'envisagerait pas le problème d'une manière interne mais prendrait en compte cinq piliers majeurs: l'alignement stratégique, la création de valeur, la gestion du risque informatique, la mesure de performance et la gestion des ressources.

CHAPITRE 3 : METHODOLOGIE DE RECHERCHE

Dans ce chapitre, nous mettrons en exergue notre modèle d'analyse qui permettra de bien mener la partie pratique de cette étude. La première partie consistera à la présentation du modèle d'analyse et la dernière partie sera consacrée aux outils de collecte et d'analyse des données.

3.1 Modèle d'analyse

Selon Jimenez & al. (2008 :55), « un modèle est une représentation schématique de tout ou une partie de l'entreprise dans un langage de représentation approprié ».

Figure 1 : Modèle d'analyse

Phases	Etapes	Outils
Préparation de l'évaluation	Prise de connaissance générale	• Entretien • Observation physique • Analyse documentaire • Questionnaire de prise de connaissance
	Description des dispositifs de sécurité du logiciel	
Evaluation des risques	Identification des risques	• Entretien • QCI • Tableau des risques • Echelle d'évaluation • Critère de cotation
	Evaluation des risques	
	Hiérarchisation et classification des risques	
Conclusion	Recommandations	• FRAP

Source : Nous-mêmes

3.2 Outils de collecte et d'analyse de données

3.2.1. Outils de collecte

Plusieurs outils existent et peuvent être combinés selon les besoins. Ceux que nous utiliserons pour la collecte des données sont les suivants : les guides d'entretien, l'observation physique et le questionnaire de prise de connaissance.

3.2.1.1 Guide d'entretien

C'est un support technique que nous avions utilisé lors des entretiens. C'est un répertoire de thèmes sur lesquels ont porté les entretiens au cours desquels les questions ont été formulées au préalable.

Cet outil est souvent celui qui est le plus difficile à conduire et celui pour lequel un débutant n'est pas préparé. Il nous a aidés à collecter des informations sur le fonctionnement du réseau informatique de l'entreprise, sur les mesures de sécurité érigées pour la sauvegarde des actifs et sur la description réelle des tâches du personnel du service informatique.

3.2.1.2 L'observation physique

Elle consiste à faire des constats visuels d'une situation afin d'en tirer des conclusions. Une bonne observation nécessite la transparence, la répétition et la validation.

Selon Renard (2010 :352), l'observation physique est un outil d'application universelle. On peut observer les processus, les biens, les documents ou les comportements. L'observation peut être directe (réalisé par l'auditeur) et conduire à un nouveau constat ou indirecte (c'est-à-dire réalisé par une tierce personne). C'est l'outil de validation par excellence lors d'une mission d'audit de sécurité informatique. Il permet de s'assurer de la réalité, de la permanence ou de la conformité des dispositifs de contrôle interne.

L'observation directe a été utilisée pour procéder à la vérification des informations recueillies par questionnaire à partir des faits et phénomènes observables directement. Elle complète

donc bien les autres techniques utilisées. Elle a eu lieu sur le site de stage et nous a permis de voir comment chacun exécute ses tâches et se comporte à son poste de travail. Les observations directes nous ont beaucoup aidé dans la connaissance de l'origine des risques qui impactent le système informatique de l'entreprise.

3.2.1.3 Questionnaire de prise de connaissance

Pour Renard (2010 :228), le questionnaire de prise de connaissance permet d'organiser la réflexion et les recherches et est indispensable :

- pour bien définir le champ d'application de sa mission ;
- pour prévoir en conséquence l'organisation du travail et en particulier en mesurer l'importance ;
- pour préparer l'élaboration des questionnaires de contrôle interne (QCI).

3.2.2 Outils d'analyse des données

3.2.2.1 Analyse documentaire

Elle consiste en l'exploitation des documents de l'organisation faisant l'objet de l'étude. Il s'agit de consulter les documents obtenus ainsi que les informations collectées afin d'avoir un aperçu de la gestion sécuritaire du réseau informatique. C'est donc une bonne technique de rapprochement pour la vérification des données.

3.2.2.2 Tableau des risques

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

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

Selon Renard (2010 :239), il sert à l'identification des risques et découpe l'activité (objet de l'audit) en tâches élémentaires. Il permet d'associer à chaque tâche les risques susceptibles de se produire et en fonction du degré d'affinement de l'analyse, il comporte 3 à 8 colonnes.

3.2.2.3 Questionnaire de contrôle interne (QCI)

D'après Rouff (2001 :15), les QCI ont pour objectifs de guider l'auditeur dans son travail d'analyse afin de lui permettre en toute objectivité, de détecter les dysfonctionnements, et d'en discerner les causes réelles.

3.2.2.4 Feuille de Révélation et d'Analyse de Problème (FRAP)

Durant la phase de terrain, pour chaque dysfonctionnement constaté, l'auditeur rédige une FRAP. Elle est un document normalisé qui va conduire et structurer le raisonnement de l'auditeur jusqu'à la formulation de la recommandation. Les FRAP serviront également de base pour la rédaction du rapport.

La FRAP reproduit les différentes phases du raisonnement dans leur ordre chronologique et logique. L'auditeur remplit une FRAP à chaque fois qu'une observation révèle un problème. En fait, l'auditeur se sert de la FRAP pour mener à bien son raisonnement.

Conclusion :

Le modèle présenté ci-dessus sera utilisé pendant la phase pratique. Les différents outils évoqués seront également indispensables pour l'évaluation des risques liés à la sécurité informatique.

Ce chapitre marque la fin de la revue de littérature et notre passage à la partie pratique.

CONCLUSION PREMIERE PARTIE

Au sein des entreprises, la sécurité des systèmes d'informations est de plus en plus abordée à l'aide d'approches basées sur les risques. L'expérience montre que de telles études réduisent de manière considérable les pertes liées aux faiblesses de sécurité des systèmes d'informations et permettent de renforcer les dispositifs de maîtrise. Cette partie nous a donc permis de comprendre l'importance de l'évaluation des risques et nous nous évertuerons donc dans les chapitres qui suivent à évaluer les risques de la SONABEL qui remettent en cause sa sécurité informatique.

DEUXIEME PARTIE : CADRE PRATIQUE

Cette seconde partie comportera concrètement l'évaluation des risques liés au logiciel ORACLE de la SONABEL. Pour y arriver, nous avons été amenés à effectuer un stage pratique au sein du service audit et du service informatique. Un état des lieux doit par conséquence être effectué afin de situer la maîtrise des risques de cet outil.

Pour atteindre cet objectif, nous allons donc à travers le chapitre 4 présenter la SONABEL et particulièrement le service informatique. Ensuite dans le chapitre 5 nous décrirons les dispositifs de sécurité mises en place. Nous terminerons par l'évaluation des risques identifiés dans le chapitre 6 suivie des recommandations.

CHAPITRE 4 : PRESENTATION DE LA SONABEL

Ce chapitre sera consacré à la présentation générale de la SONABEL. Il comporte trois parties, la première qui relatera l'historique de la SONABEL et quelques chiffres pertinents, la seconde comportera la présentation de ses missions, sa vision et son organisation. La dernière sera réservée à la présentation des départements audit et contrôle de gestion, et informatique car nous avons été affecté dans ces lieux durant notre séjour à la SONABEL.

4.1 Historique et quelques chiffres pertinents

4.1.1 Historique

La Société Nationale d'Electricité du Burkina (SONABEL) est une société d'Etat au capital de soixante trois milliards trois cent huit millions deux cent soixante dix mille (63 308 270 000) francs CFA. Elle a son siège social à Ouagadougou, Avenue de la Nation, 01 BP 54 Ouagadougou 01. Avant de devenir en 1976 un Etablissement Public à caractère Industriel et Commercial (EPIC), la SONABEL a connu de nombreuses transformations tant au niveau de sa structure financière (capital) qu'au niveau de sa dénomination.

Elle fut appelée successivement Energie de l'Afrique Occidentale Française (Energie AOF) qui était une société privée française puis Société Africaine d'Electricité (SAFELEC), ensuite Société Voltaïque d'Electricité (VOLTELEC).

- 1954 : l'électricité AOF débute l'activité de production et de distribution de l'énergie électrique à Ouagadougou et à Bobo-Dioulasso respectivement en février et octobre 1954;
- 05 mars 1956 : extension de l'activité à la distribution d'eau dans les deux villes;
- 1960 : reprise de l'ensemble des activités par la société d'économie mixte multinationale SAFELEC, au capital de 150 millions de francs CFA réparti entre la Caisse Centrale de Coopération Economique (CCCE), actuelle Agence Française de Développement (AFD) d'une part, la Haute-Volta, le Niger, la Mauritanie et divers actionnaires privés d'autre part;
- 06 septembre 1968 : la société prend la forme de société anonyme de droit voltaïque (VOLTELEC) dont le capital social de un million de francs CFA

réparti entre la CCCE, la SAFELEC et les personnalités voltaïques;

- 1970 : Abandon de la distribution d'eau par la VOLTELEC au profit de la Société Nationale des Eaux (SNE) actuelle ONEA;
- 15 septembre 1976 : la VOLTELEC prend la forme d' Etablissement Public à Caractère Industriel et Commercial (EPIC) par décret n°76/344/PRES/MTP/URB avec un capital de 1 387 628 180 francs CFA; dans la même année, par ordonnance n°76/021/PRES/URB, l'exclusivité de la production, du transport et de la distribution de l'électricité lui fut accordée;
- En août 1984, avec l'avènement du Conseil National de la Révolution (CNR) et le changement du nom du pays, la VOLTELEC a pris le nom de Société Nationale d'Electricité du Burkina en abrégé SONABEL.

4.1.2 quelques chiffres pertinents

Le tableau ci-dessous montre l'évolution de la SONABEL durant les quatre dernières années :

Tableau 3 : Chiffres clés de la SONABEL

	Année 2010	Année 2011	Année 2012	Année 2013
Capital en Francs CFA	63 308 270 000	63 308 270 000	63 308 270 000	63 308 270 000
Effectif du personnel	1495	1 530	1 510	1 610
Nombres d'abonnés desservis en BT	361092	400 356	434 985	471 097
Nombres d'abonnés desservis en MT	1073	1 120	1 218	1 344
Chiffre d'affaires	93 600 678	99 933 451	112 059 077	122 077 541
Nombre de branchements	33 780	42 129	37 360	43 998

Source : Rapports d'activités de la SONABEL (2010, 2011, 2012,2013)

4.2 Structure organisationnelle, missions et vision de la SONABEL

4.2.1. Structure organisationnelle

Afin d'assurer une conformité des titres avec ceux des Sociétés d'électricité de la sous- région et des sociétés d'Etat du Burkina Faso, les dénominations des niveaux hiérarchiques retenues sont les suivantes :

- Directeur Général ;
- directeurs centraux ;
- chefs de départements et directeurs régionaux ;
- chefs de services ;
- chefs de divisions ;
- chefs de sections.

La SONABEL a à sa tête un Conseil d'Administration qui est composé de neuf (09) membres et qui sont nommés par décret pris en conseil de Ministres.

Au titre des directions, nous avons :

- une Direction Générale ;
- une Direction des Etudes, de la Planification et de l'Equipement ;
- une Direction de la production ;
- une Direction du transport ;
- une Direction commerciale et de la clientèle ;
- une Direction de la Distribution ;
- une Direction des Finances et de la Comptabilité ;
- une Direction des Marchés et du Patrimoine ;
- une Direction des Ressources Humaines.

Ces directions sont organisées en départements, services, divisions et sections.
Le Directeur Général est assisté de Conseiller(s) et d'un(e) Assistant(e) de Direction qui sont nommés par décision du Directeur Général.

Les Départements rattachés à la direction générale sont :

- département de la Communication, des Archives et de la Documentation ;
- département Qualité – Environnement – Sécurité ;
- département Audit et Contrôle de Gestion ;
- département Informatique ;
- département Juridique.

4.2.2 Missions

La Société Nationale d'Electricité du Burkina est une société d'Etat qui a reçu des pouvoirs publics, les missions suivantes :

- la production, le transport, la distribution et l'importation de l'électricité sur l'ensemble du territoire national ;
- la desserte des populations des villes et des campagnes en quantité suffisante d'électricité de bonne qualité et à un prix raisonnable ;
- l'appui au développement industriel et économique du pays ;
- la rentabilité des capitaux mis à sa disposition et/ ou crées par elle-même.

Cependant, pour atteindre ces objectifs, les missions suivantes ont été assignées à chacune de ses directions :

– direction générale :

Les pouvoirs attribués au Directeur Général sont les suivants :

- il a qualité d'ordonnateur du budget de la société. Il peut déléguer sous sa responsabilité une partie de ses pouvoirs en la matière ;
- il est chargé de la direction technique, administrative et financière de la société qu'il représente dans les actes de la vie civile, notamment à l'égard des tiers et des usagers ;
- il peut ester en justice au nom de la société ;
- il prépare les délibérations du Conseil d'Administration et en exécute les décisions ;
- il signe les actes concernant la société, toutefois il peut donner à cet effet toutes délégations nécessaires sous sa propre responsabilité ;
- il nomme et révoque tout agent ou employé conformément à la réglementation en vigueur ;

- il paye les salaires et émoluments conformément aux textes en vigueur dans le secteur.

– la direction des études, de la planification et de l'équipement a pour missions de:

- proposer à la direction générale les plans stratégique et opérationnel de la SONABEL ;
- réaliser des études économiques, financières et statistiques en rapport avec les schémas directeurs et les projets d'investissements de la société ;
- fournir l'expertise et le support technique pour l'élaboration des normes, standards et méthodes de travail dans l'optique d'une utilisation optimale des ressources humaines, financières et matérielles ;
- élaborer le plan d'investissement de la société ;
- élaborer des fiches de projet pour la recherche de financements ;
- maintenir la base de données à jour des différents plans et des immobilisations issus des investissements ;
- assurer l'exercice de la veille technologique ;
- veiller au bon fonctionnement des processus placés sous sa responsabilité ;
- préparer les dossiers d'appel d'offres se rapportant à l'exécution du budget de la direction.

– La direction de la production

Elle a en charge les principales missions ci-après :

- produire l'électricité au moindre coût, avec le niveau de qualité attendu, en vue de contribuer à la satisfaction de la demande d'électricité tout en assurant la durée de vie optimale du parc de production ;
- assurer la maintenance et le suivi technique des installations de protection.

– La direction du transport

Elle a en charge les principales missions ci-après :

- transporter l'électricité avec le niveau de qualité attendu tout en assurant la surveillance et l'entretien du réseau dans une optique de continuité du service et de durée de vie optimale des ouvrages ;
- assurer les mouvements d'énergie sur le réseau de transport d'électricité au moindre coût et selon la qualité attendue ;
- assurer le bon fonctionnement et la disponibilité des dispositifs de relayage, régulation, protection et télécommunication.

– La direction commerciale et de la clientèle :

- élaborer la politique et les stratégies dans le domaine de la gestion commerciale et du processus clientèle en vue de sauvegarder les intérêts de l'entreprise et d'assurer la satisfaction de la clientèle ;
- assurer un appui technique aux services gestion clientèle des directions régionales ;
- gérer la clientèle d'affaires et veiller à son recouvrement ainsi que les clients de l'administration, des collectivités et du secteur privé ;
- fournir des services à la clientèle de la SONABEL au niveau régional de façon à répondre à leurs besoins à moindre coût ;
- assurer les étalonnages des compteurs et autres appareils de mesure de la distribution.

– La direction de la distribution

Elle a pour attribution de :

- proposer à la Direction Générale l'ensemble des stratégies, politiques et directives dans le domaine de la distribution et s'assurer de leur application ;
- assurer les services de la distribution d'électricité, contrôler la qualité de la fourniture sur tout le territoire national, contrôler l'application des consignes de sécurité, la gestion des statistiques d'exploitation et des plans des réseaux de distribution ;
- fournir aux clients une alimentation électrique fiable et continue.

- La direction des marchés et du patrimoine
    - gérer les services administratifs et généraux ainsi que les baux immobiliers ;
    - gérer le patrimoine et veiller à l'élaboration et à la mise à jour de la mise en place des procédures administratives et des notes d'organisation ;
    - gérer les approvisionnements de matériel et fournitures d'exploitation et d'entretien dans les meilleures conditions de qualité, de prix et de délais ;
    - assurer et/ou vérifier la rédaction des contrats et autres conventions et des marchés ;
    - assister les directions opérationnelles dans les négociations des contrats et dans la rédaction des clauses juridiques des différents documents contractuels dont il en assure la garde.

- La direction des finances et de la comptabilité
    - proposer à la direction générale l'ensemble des stratégies, politiques, directives et programmes de gestion budgétaire, financière et comptable et s'assurer de leur application ;
    - fournir les données financières et comptables fiables en temps opportun ;
    - proposer à la direction générale la charte de délégation des pouvoirs administratifs et financiers, les procédures administratives en découlant et en assurer l'application.

- La direction des ressources humaines
    - proposer à la direction générale l'ensemble des stratégies, politiques, directives et programmes de gestion des ressources humaines et d'organisation et de s'assurer de leur application ;
    - conseiller la direction générale dans les prises de décisions en matière de gestion des ressources humaines et d'organisation ;
    - fournir à l'ensemble de la société des services relatifs à la gestion des ressources humaines et à l'organisation ;

- fournir l'expertise et le support pour l'élaboration de solutions aux problèmes de santé et de conditions de travail.

4.2.3 Objectif de la SONABEL

A l'image des grandes entreprises modernes, la SONABEL s'est dotée d'une vision qui lui servira de repère dans son évolution. Cette vision voudrait faire de la SONABEL, l'acteur majeur de la transformation du sous secteur de l'électricité au Burkina-Faso focalisé sur l'approvisionnement et la sécurité de la fourniture d'énergie électrique au meilleur coût, avec l'objectif permanent :

- d'améliorer l'accès à l'électricité des burkinabés et en portant le taux d'électrification à 40% ;
- de délivrer des services de qualité à ses clients ;
- d'accompagner le développement économique et partant, la lutte contre la pauvreté dans le pays.

La réalisation de cette vision repose sur les piliers majeurs suivants :

- développer la rentabilité ;
- mettre l'organisation au service du client (accueil, satisfaction de ses besoins, service commercial) ;
- mobiliser et développer la satisfaction du personnel autour de cette vision.

4.3 Présentation des départements

4.3.1 Présentation du département audit et contrôle de gestion

Ce département est chargé de :

- concevoir les procédures pour assurer la transparence des opérations et l'exactitude des transactions ;
- contrôler, mesurer et analyser l'activité de l'entreprise ;
- apporter au directeur général à travers un système d'informations fiables, les éléments essentiels pour le management de l'entreprise ;
- réaliser un contrôle de vérification en vue de déterminer les indicateurs de gestion technique, commerciale, comptable et financière pertinents ;

- veiller au reporting de l'analyse des résultats de l'entreprise pour le Directeur Général et du suivi de son exécution ;
- suivre les tendances et l'évolution des résultats par rapport aux prévisions du modèle financier de la SONABEL.

Il comprend deux (02) services : le Service Audit Interne et le Service Contrôle de Gestion.

4.3.2 Présentation du département informatique

Ce département, initialement logé à la Direction Financière et Comptable, est dorénavant rattaché à la Direction Générale par sa transversalité; ce qui lui permet de jouer pleinement son rôle de fournisseur aux autres directions. La restructuration de ce département s'est traduite par la création d'autres services pour tenir compte de l'évolution du système d'information et de la croissance de la société.

Il comprend en tout quatre (04) services :

- le Service Application Informatique;
- le Service Infrastructure et Réseau;
- le Service Support aux Utilisateurs;
- le Service de Traitement Informatique des Régions.

4.3.1 Le Service Applications Informatiques

Le Service Applications Informatiques a pour attributions de :

- définir l'architecture fonctionnelle et applicative des systèmes d'informations ;
- concevoir et intégrer les composants applicatifs ;
- faire la maintenance applicative, corrective et évolutive ;
- mettre en exploitation et gérer les serveurs, les bases de données et applications ;
- gérer la sécurité, les performances et optimiser les bases de données et les applications.

4.3.2 Le Service Infrastructure et Réseau

Le Service Infrastructure et Réseau a pour attributions de :

- inventorier et gérer les infrastructures (équipements et réseaux) ;

- gérer la téléphonie ;
- gérer les accès et les performances ;
- installer les infrastructures et gérer les mises à jour ;
- gérer les évolutions et la maintenance des infrastructures ;
- assister et conseiller les utilisateurs ;
- gérer la sécurité de l'infrastructure ;
- définir et superviser la politique sécurité du système d'information ;
- évaluer et analyser les risques ;
- étudier les moyens et préconisations ;
- auditer et contrôler la mise en œuvre de la politique du système d'information ;
- sensibiliser et former aux enjeux de la sécurité du système d'information.

4.3.3 Le Service Support aux Utilisateurs

Le Service Support aux Utilisateurs a pour attributions d'accueillir, enregistrer et suivre les demandes d'intervention, de traiter ou déclencher les actions de support correspondantes, de former et aider à la prise en main des équipements et logiciels installés et d'analyser et suivre les besoins des utilisateurs.

4.3.4 Le Service Traitement Informatique des Régions

Il a pour attributions d'administrer le système informatique de la direction régionale, d'apporter une assistance technique aux utilisateurs et d'assurer la maintenance du parc informatique.

Conclusion :

Cette présentation nous a permis de comprendre l'organisation de la SONABEL, son fonctionnement et de mieux appréhender le département informatique.
A la suite de cette étape, la description des dispositifs de sécurité existants fera l'objet de notre prochain chapitre.

CHAPITRE 5 : DESCRIPTION DES LOGICIELS ET DES DISPOSITIFS DE SECURITE

Ce chapitre décrira premièrement les différents logiciels utilisés par la SONABEL, ensuite une brève présentation du logiciel Oracle qui est l'objet de notre étude et nous terminerons par la description des dispositifs de sécurité au niveau du logiciel Oracle.

5.1 Les applications métiers et les divers logiciels de la SONABEL

5.1.1 La gestion clientèle (GESCLI)

C'est l'application qui permet la facturation des consommations d'électricité des clients et leur prise en charge depuis l'abonnement jusqu'à la résiliation le cas échéant. Ce système assure la gestion du portefeuille des abonnés basse tension particuliers ainsi que les clients de l'administration basse et haute tension double tarif. Quant aux clients particuliers basse et haute tension double tarif, seule leur facturation est faite par GESCLI, les encaissements étant gérés au niveau d'un autre logiciel. GESCLI permet d'éditer les différents états de base pour une prise en charge adéquate dans la comptabilité de la SONABEL.
Elle a été conçue et développée par le département informatique avec un système de gestion de base de données oracle. Le département informatique demeure le support technique, assure la maintenance et les mises à jour.

5.1.2 La paye

C'est un progiciel pour l'administration des carrières du personnel et le calcul des rémunérations. Il est utilisé principalement par le Département Administration du Personnel.

5.1.3 Le SIGEST

C'est le système d'information de gestion. Il rassemble toutes les données utilisées par la SONABEL, et permet d'élaborer des statistiques sur la production d'électricité, les ventes, les consommations des fuels et de rédiger un tableau de bord à tout instant. C'est un outil d'aide à la décision. Il intègre aussi un module de gestion de compétences à travers la prise en compte des formations du personnel. Il est utilisé par l'ensemble des Directions. Le Département

Informatique assure son développement, en collaboration avec le Département des Etudes et de la Planification, et sa maintenance.

5.1.4 Eclipse et Cash Power

Ces deux progiciels sont des systèmes de prépaiement d'électricité. Ces applications permettent l'achat des unités par les consommateurs pour recharger leurs compteurs électriques. Ils sont utilisés par la Direction Régionale du Kadiogo, la Direction Régionale de l'Ouest et la Direction Régionale du Centre Ouest. Le Département Informatique assure le support technique.

5.1.5 Les logiciels de bureautique et les systèmes d'exploitation

Le système de messagerie interne est Lotus Domino. C'est un outil collaboratif qui intègre des modules de gestion de courriers, d'agendas, de tâches et de logiciel de traitement de texte (Symphony).
Les logiciels de bureautique utilisés sont Office 2000/2003 et OpenOffice.
Les postes de travail sont équipés de systèmes d'exploitation Windows 2000/XP/Vista.

5.1.6 La messagerie externe et les services internet

Le système de messagerie externe est géré par postfix. C'est un logiciel libre qui tourne sur un serveur linux ubuntu. Les messages entrants et sortants sont analysés grâce à l'antivirus kaspersky.
Les services internet fournis par la SONABEL sont le web, le DNS. Un serveur proxy gère l'accès à internet. Les serveurs supportant ces services orientés internet sont dans la DMZ.

5.1.7 Oracle Applications

C'est une suite d'applications qui permet de gérer la comptabilité, les bons de commande et la gestion de stocks. Elle est utilisée par l'ensemble des départements pour initier des demandes d'achat. Mais c'est essentiellement, le Département Comptable, le Département des finances et le Département Gestion des Approvisionnements qui l'utilisent. Le Département

Informatique assure la maintenance. Ce dernier fera l'objet de notre étude dans les parties suivantes.

5.2 Présentation du logiciel Oracle Applications

Oracle Applications fait partie de la catégorie des progiciels de gestion intégrée (ERP). Depuis son acquisition ORACLE est un logiciel qui permet à la SONABEL d'obtenir de son système d'information les informations les plus récentes et précises. Il l'aide également à placer l'information au cœur de son activité en suivant trois principes : simplifier, normaliser et automatiser. Ces principes permettent à la SONABEL d'utiliser des informations de grande qualité pour collaborer, mesurer les résultats pour s'améliorer en permanence.

5.2.1 Les versions d'Oracle Applications

Oracle Applications a été acquis en 2001 avec la version 11.0.3 par le cabinet Price Water Cooper House basé en côte d'ivoire. Suite à des difficultés causées par un manque d'assistance technique, une migration vers la version 11i en 2008-2009 a été faite par le cabinet CATALYS situé au Maroc.
Dans les années à venir la SONABEL prévoit une fois de plus une migration vers la version R12 pour une meilleure utilisation.

5.2.2 Les composants d'Oracle Applications

Oracle Applications possède deux bases :

- la base de test qui comme son nom l'indique sert à faire des tests, des essais ou des simulations. Une copie de la base réelle est faite sur la base de test chaque année et à chaque fois que cela est nécessaire. S'il survient quelques problèmes au niveau du système, les solutions pour y remédier sont d'abord testées dans cette base ;
- la base d'exploitation réelle : c'est celle dans laquelle travaillent tous les utilisateurs.

5.2.3 Les fonctionnalités d'Oracle Applications

Oracle permet d'assurer :

- la manipulation des données ;
- la cohérence des données ;
- la confidentialité des données ;
- l'intégrité des données ;
- la sauvegarde et la restauration des données.

5.2.4 Les modules d'Oracle Applications

La SONABEL n'a pas besoin de la gamme complète des modules d'Oracle. Elle en utilise cinq (5) subdivisés en deux (2) parties que sont :

- l'environnement des finances composé des trois (03) premiers modules acquis en 2001 :
  - la comptabilité générale
  - la gestion des fournisseurs
  - la gestion des immobilisations
- l'environnement logistique qui comprend les deux (02) derniers modules acquis en 2003-2004 :
  - la gestion des achats
  - la gestion des stocks

Un module supplémentaire nommé accounting global engine est chargé de faire la traduction des écritures comptables des quatre (04) autres modules vers celui de la comptabilité générale.

5.2.5 Interface d'Oracle Applications

Une interface a été réalisée entre le logiciel Oracle et ceux de la gestion clientèle et de la paye. Pour les directions régionales, leurs données sont récupérées par clé USB dans le but de les traduire en écritures comptables et insérer dans la base de données d'Oracle.

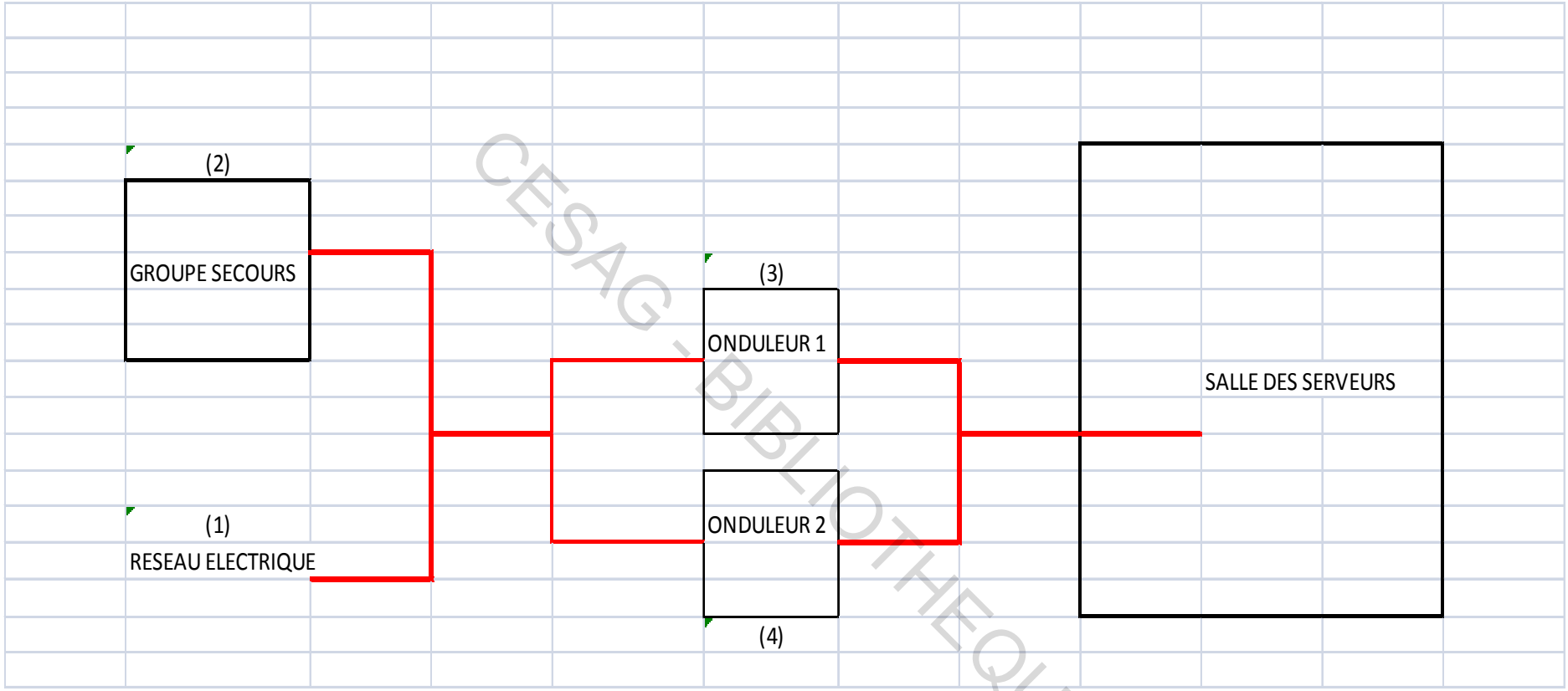
5.3 Description des dispositifs de sécurité

A travers les entretiens et les observations au cours de notre stage, nous avons pu identifier les procédures de sécurité mises en place. Nous décrirons premièrement la sécurité physique, ensuite la sécurité du réseau au sein de la SONABEL et nous terminerons par les dispositions prises pour sécuriser le logiciel Oracle.

5.3.1 Sécurité physique

L'accès aux salles informatiques se fait par des badges ou empreintes digitales. Seul le personnel informatique est autorisé à accéder à ces zones. Un système de détection et d'extinction automatique d'incendie a été installé dans la salle des serveurs. Le circuit électrique mis en place permet la continuité de la fourniture d'électricité. Ce circuit est composé d'un groupe électrogène de secours et de deux onduleurs d'une autonomie d'au moins une heure (1h) de temps chacun. En cas de coupure, le groupe électrogène assure la relève jusqu'au rétablissement de l'électricité. Si à un certain moment par exemple, le groupe ne fonctionne plus, le premier onduleur fournit l'électricité et ensuite le deuxième. Ce qui empêche l'interruption des serveurs et permet la stabilité du courant.
Un serveur de secours en hot line avec le serveur principal délocalisé à 5km du siège est disponible en cas de panne. De même, des systèmes de climatisation maintiennent l'environnement dans des conditions idéales de fonctionnement.

Figure 2 : Circuit électrique pour la continuité de la fourniture d'électricité de la salle des serveurs



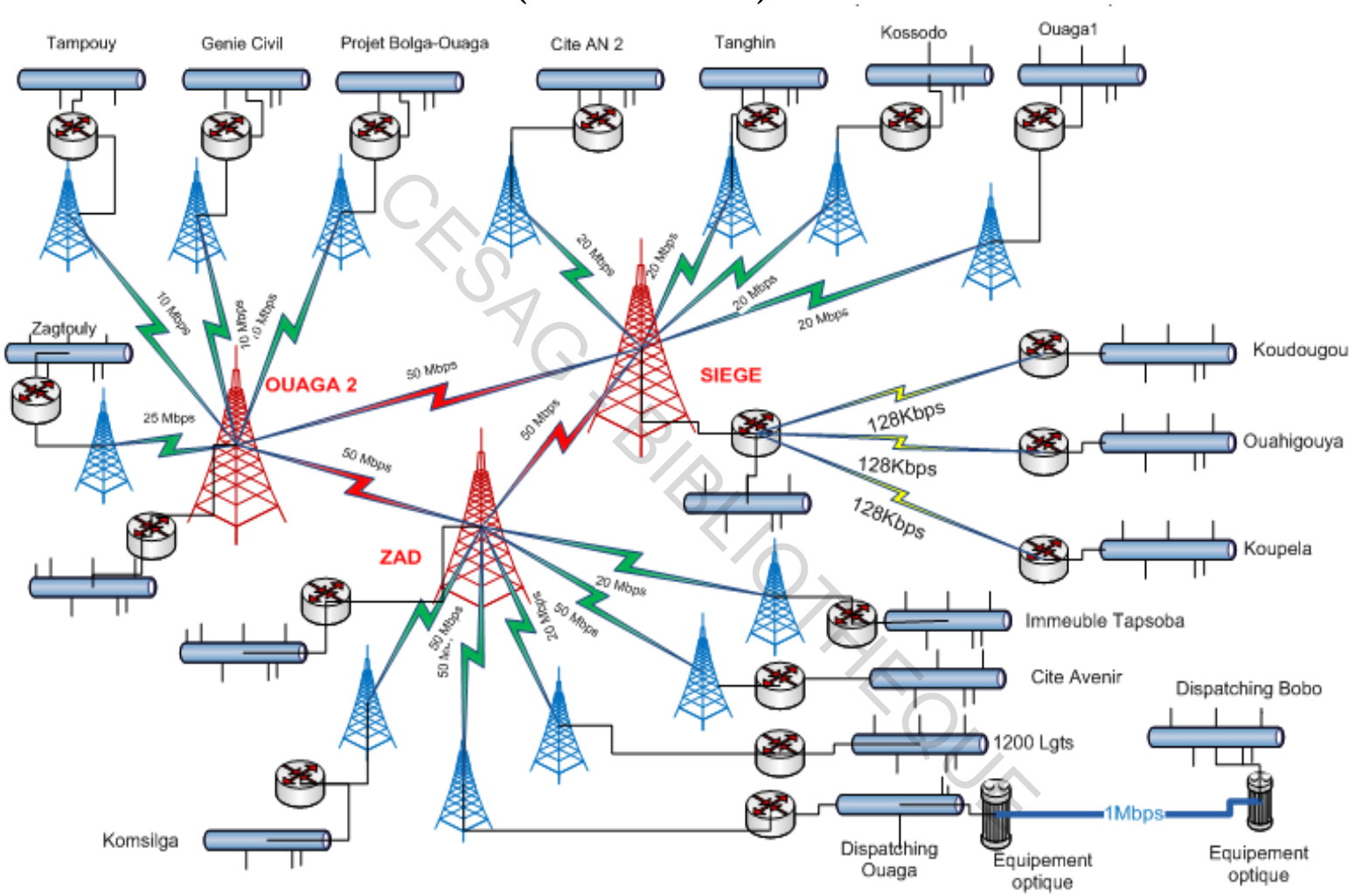
Source: Nous-mêmes

5.3.2 Sécurité du réseau

Le réseau informatique de la SONABEL est un WAN (Wide Area Network) composé d'un réseau central, qui se trouve au siège, auquel viennent se connecter, via des liaisons filaires ou sans fil, les réseaux locaux des différents sites de la société. Autour de ce WAN, d'autres réseaux locaux des localités isolées s'y interconnectent momentanément à travers des modems utilisant les lignes téléphoniques analogiques.

Ce réseau est protégé par un pare-feu ou firewall contrôlant les communications qui le traversent et dispose d'un système de détection d'intrusion. Le réseau du siège est un réseau local unique segmenté en cinq réseaux locaux virtuels ou VLAN (Virtual Local Area Network) c'est-à-dire que le réseau regroupe un ensemble de machines de façon logique et non physique. En d'autres termes cela signifie qu'il existe une séparation des utilisateurs en fonction de leurs activités. L'avantage à ce niveau c'est qu'il conduit à une séparation des risques. Ces VLAN sont également connectés à internet à travers un pare-feu.

Figure 3 : Schéma du réseau WAN de la SONABEL (OUAGADOUGOU)



Source : nous-mêmes

5.3.3 Sécurité logique

Nous allons décrire ici les mécanismes de sécurité mis en place par la SONABEL pour assurer l'intégrité, la confidentialité et la disponibilité des données d'Oracle.

5.3.3.1 Gestion des mots de passe et des comptes utilisateurs

L'accès au logiciel Oracle est authentifié par un compte d'utilisateur et un mot de passe. Avant 2009 le compte était composé du prénom de l'utilisateur et de l'abréviation du nom. S'étant rendue compte que la SONABEL paye plus de licences lorsque le nombre d'utilisateurs augmente, il a été décidé après 2009 que les fonctions des personnes concernées soient utilisées comme nom d'utilisateur.

Il n'existe aucun gestionnaire de mots de passe. Les utilisateurs en sont responsables et chacun gère son mot de passe à sa guise. Le risque de vol de mots de passe est donc élevé car ils ne sont pas changés régulièrement.

Au-delà de 15 à 20 minutes, si l'application reste inactive le système se ferme automatiquement pour éviter certaines tentatives.

5.3.3.2 Prévention, détection et neutralisation des logiciels malveillants

La SONABEL dispose d'un antivirus KASPERSKY avec une mise à jour automatique mais les licences sont expirées sur tous les postes. Aucun utilisateur n'a le droit d'installer d'autres logiciels.

5.3.3.3 sauvegardes et stockage des données

La sauvegarde des données est faite automatiquement toutes les nuits à 1h00. Les données étaient stockées auparavant sur des petites bandes de 1Go. Suite à une évolution très rapide des données, le stockage se fait désormais en interne sur un disque qui se trouve dans la même salle que le serveur.

La SONABEL a subi récemment un cas de perte de données sur le serveur principal. Les informaticiens ayant voulu restaurer les sauvegardes se sont rendu compte que les données des trois (3) derniers jours n'ont pas été sauvegardées sur le disque. Cela s'explique par le fait

que la capacité du disque était devenue insuffisante. Pour récupérer les données déjà perdues de cette période, les saisies ont été reprises manuellement en l'attente d'une remise en service du système informatique.

5.3.3.4 Plan de continuité de l'activité

Les dispositions prises par la SONABEL pour assurer la continuité des activités en cas de survenance d'un problème sont les suivantes :

- la sauvegarde des données ;
- redondance des onduleurs : en cas de première urgence, des alimentations de secours (onduleurs) préservent le fonctionnement du système pendant plus d'une heure laissant ainsi le temps de réparer la panne électrique ou de fermer les applications ;
- la redondance des serveurs : lorsque le principal est hors service, le serveur de secours prend le relais ;
- l'existence d'un groupe électrogène en cas de besoin.

Conclusion :

Ce chapitre nous a permis d'avoir une idée sur la sécurité informatique de la SONABEL et de pouvoir cerner les zones à risques concernant essentiellement le logiciel Oracle. Pour mieux étudier et évaluer ces risques nous passerons donc au chapitre suivant.

CHAPITRE 6 : EVALUATION DES RISQUES LIES AU LOGICIEL ORACLE ET RECOMMANDATIONS

Dans ce chapitre nous identifierons tout d'abord, les risques potentiels liés au logiciel, puis nous procéderons à l'évaluation et à l' hiérarchisation de ces risques en fonction de leur probabilité de survenance et de leur gravité. Enfin, nous dégagerons les recommandations à travers l'analyse des forces et faiblesses**.**

6.1 Identification des risques liés au logiciel Oracle

Nous avons retenu l'identification par découpage de l'activité en tâches élémentaires parmi les techniques d'identifications présentées au chapitre 2. Ce découpage permettra de s'assurer que les tâches sont bien exécutées. L'identification se fera à travers un tableau de six (6) colonnes qui contient :

- les différentes tâches ;
- les objectifs du contrôle ;
- les risques identifiés ;
- les impacts du risque ;
- les dispositifs qui permettent de maitriser le risque ;
- l'existence de ces dispositifs.

Tableau 4 : Identification des risques

Tâches	Objectifs	Risques	Impacts	Dispositifs de sécurité	Existence du dispositif
Gestion de la sécurité physique	S'assurer de l'accès des locaux informatiques par le personnel autorisé	- Vol du matériel informatique - Accès non autorisé	Dommage ou destruction physique des SI	- Accès par badge - Service de gardiennage - Détection d'intrusion - Accès par empreinte digitale - Vidéo surveillance	oui non non oui non
	S'assurer de la protection de tous les actifs informatiques	- Incendie - Risque électrique - Coupure d'électricité	- Indisponibilité du SI - Destruction de données - Destruction des bâtiments	- Groupe électrogène - Onduleurs avec batterie - Extincteur automatique - Contrat d'assurance du matériel	oui oui oui oui
	S'assurer que les incidents environnementaux n'ont qu'un faible impact sur l'activité	- Inondation - Poussière - Chaleur / humidité	- Dommage ou destruction physique des SI - Destruction de données - Indisponibilité du SI	- Salles situées en hauteur - Service de nettoyage - Climatisation adéquate	non oui oui

Gestion de la sécurité des réseaux	S'assurer de la sécurité des échanges effectués sur le réseau	- Exposition aux attaques des virus - Attaques des cybers pirates - Divulgation d'informations confidentielles - Tentative d'accès non autorisé	- Modification des données - Ralentissement des traitements - Destructions des données - Accès non autorisé - Copie des données - Non disponibilité du SI	- Système de détection d'intrusion - Segmentation du réseau local virtuel - Pare-feu - Antivirus - Cryptographie - Serveur proxy	oui oui oui oui oui oui
Gestion des mots de passe et comptes utilisateurs d'Oracle	S'assurer de la protection des données	– Divulgations d'informations confidentielles – Vol de mot de passe – Accès non autorisé – Saisie faussée de données	– Perte de confidentialité – Modification de données – Copie de données – Perte d'intégrité	– Accès par mot de passe – Accès par compte d'utilisateur – Renouvellement fréquent des mots de passe – Gestionnaire de mots de passe	oui oui non non
Prévention, détection et neutralisation des logiciels malveillants	S'assurer de la protection des accès au logiciel	– Exposition aux attaques de virus – Faille de sécurité – Contre-mesure inefficace	– Dysfonctionnement du logiciel – Altération des données	– Logiciel antivirus – Renouvellement des licences – Limitations des téléchargements – Interdiction d'installer d'autres logiciels	oui non non oui

Sauvegarde et stockage des données	S'assurer de la confidentialité, de l'intégrité et de la disponibilité des données	– Erreur dans l'entrée des données – Erreur de manipulation – Erreur de programmation – Panne d'électricité – Perte de données Désastre environnemental	– Données erronées – Modification de données – Reprise des saisies – non-disponibilité du SI – destructions des infrastructures informatiques	– Procédure de sauvegarde définie – Sauvegarde régulière – Stockage des données hors site (externe) – Procédure d'archivage – Test de restauration occasionnel	oui oui non non non
Plan de continuité de l'activité	S'assurer de la continuité de l'activité en cas de panne	– Panne matérielle – Interruption du logiciel – Arrêt de l'activité Reprise d'activité compromise	– Perte de données – Difficulté de récupération	– Serveur de secours – Groupe électrogène – Plan de sauvegarde – Plan de secours informatique – Duplication des données sur un autre site – Contrat d'assurance du matériel – Archivage électronique	oui oui oui oui non oui non

Source : Nous-mêmes, à partir de Renard (2010 :239)

6.2 Evaluation des risques identifiés

Pour évaluer le niveau d'un risque, on détermine la probabilité d'occurrence du risque et le niveau de gravité de ses conséquences. Cette évaluation tiendra compte seulement des risques identifiés dans le tableau ci-dessus.

6.2.1 Evaluation selon la probabilité de survenance des risques identifiés

En fonction des dispositifs de sécurité au chapitre 5, nous déterminerons les probabilités de survenance des risques identifiés à partir d'une échelle. Cette échelle est définie par des niveaux allant de 1 à 5 pour mesurer la probabilité de survenance, et par des critères que nous avons déterminé qui se présente dans le tableau ci-dessous.

Tableau 5 : Echelle d'évaluation de la probabilité de survenance des risques

Niveau	Cote	Critères
Très forte	5	Il est extrêmement probable que le risque se produise
Forte	4	Il est très probable que le risque se produise
Moyen	3	Il est probable que le risque se produise
Faible	2	Il est peu probable que le risque se produise
Très faible	1	Il est très rare que le risque se produise

Source : Nous-mêmes

Tableau 6 : Evaluation selon la probabilité de survenance

Risques	Niveau	Cote	Commentaires
R1.Accèsnon autorisé aux locaux informatiques	Très forte	5	négligence des agents informatiques
R2. Vol du matériel informatique	Forte	4	Absence de contrôle
R3. Incendie	Faible	1	défaillance du dispositif de sécurité
R4. Incidents électriques	Moyen	3	défaillance du dispositif de sécurité
R5. Coupure d'électricité	Faible	2	défaillance du dispositif de sécurité
R6. Inondations	Faible	2	Salle non située en hauteur
R7. Poussière	Faible	2	Absence de contrôle
R8. Chaleur / Humidité	Faible	2	Absence de contrôle
R9. Exposition aux attaques de virus	Moyen	3	défaillance du dispositif de sécurité
R10. Accès non autorisé au réseau	Très faible	1	défaillance du dispositif de sécurité
R11. Attaques des cybers pirates	Très faible	1	défaillance du dispositif de sécurité
R12. Vol de mot de passe	Moyen	4	Absence de contrôle
R13.Divulgationsd'informations confidentielles	Faible	2	Absence de contrôle
R14. Accès non autorisé au logiciel	Moyen	3	Absence de contrôle
R15. Saisie faussée de données	Moyen	4	Absence de contrôle
R16. Faille de sécurité	Très faible	1	défaillance du dispositif de sécurité
R17. Contre-mesure inefficace	Très faible	1	défaillance du dispositif de sécurité
R18. Erreur dans l'entrée des données	Faible	2	manque d'attention
R19. Erreur de manipulation	Faible	2	manque d'attention
R20. Erreur de programmation	Faible	2	défaillance du dispositif de sécurité
R21. Perte de données	Faible	2	défaillance du dispositif de sécurité
R22. Désastre environnemental	Très faible	1	Absence de contrôle
R23. Panne matérielle	Faible	2	Absence de contrôle
R24. Interruption du logiciel	Faible	2	défaillance du dispositif de sécurité
R25. Arrêt de l'activité	Faible	2	défaillance du dispositif de sécurité
R26. Reprise d'activité compromise	Faible	2	défaillance du dispositif de sécurité

Source : Nous-mêmes

Les cotes dans ce tableau sont retenues en fonction de l'efficacité du dispositif de sécurité existant, de l'exploitation des documents, de notre observation physique et en tenant aussi compte de nos critères d'appréciation définis dans le tableau 5.

6.2.2 Evaluation selon la gravité des risques identifiés

La gravité ici mesure l'importance des conséquences qui ont un impact négatif sur la SONABEL, en cas de survenance des risques identifiés. Nous allons donc définir des critères de cotation de la gravité dans le tableau suivant :

Tableau 7 : Echelle d'évaluation de la gravité

Niveau d'impact	Cote	Critères
Très grave	5	Conséquences très importantes qui peuvent mettre en cause la survie de l'entreprise
Grave	4	Conséquences importantes qui peuvent entrainer l'arrêt des activités pendant quelques jours
Moyennement grave	3	Conséquences significatives qui peuvent empêcher le fonctionnement d'un service
Peu grave	2	Conséquences faibles qui peuvent bloquer certaines activités pendant quelques heures
Insignifiant	1	Conséquences très négligeables qui n'ont aucun impact sur les activités

Source : Nous-mêmes

Tableau 8 : Evaluation de la gravité

Risques	Niveau	Cote	Commentaires
R1.Accèsnonautoriséauxlocauxinformatiques	Très grave	5	négligence des agents informatiques
R2. Vol du matériel informatique	Grave	4	Absence de contrôle
R3. Incendie	Très grave	5	défaillance du dispositif de sécurité
R4. Incidents électriques	Moyennement grave	3	défaillance du dispositif de sécurité
R5. Coupure d'électricité	Moyennement grave	3	défaillance du dispositif de sécurité
R6. Inondations	Très grave	5	Salle non située en hauteur
R7. Poussière	Peu grave	2	Absence de contrôle
R8. Chaleur / Humidité	Moyennement grave	2	Absence de contrôle
R9. Exposition aux attaques de virus	Moyennement grave	3	défaillance du dispositif de sécurité
R10. Accès non autorisé au réseau	Très grave	5	défaillance du dispositif de sécurité
R11. Attaque des cybers pirates	Très grave	5	défaillance du dispositif de sécurité
R12. Vol de mot de passe	Grave	4	Absence de contrôle
R13. Divulgations d'informations confidentielles	Grave	5	Absence de contrôle
R14. Accès non autorisé au logiciel	Très grave	5	Absence de contrôle
R15. Saisie faussée de données	Grave	4	Absence de contrôle
R16. Faille de sécurité	Grave	4	défaillance du dispositif de sécurité
R17. Contre-mesure inefficace	Grave	4	défaillance du dispositif de sécurité
R18. Erreur dans l'entrée des données	Peu grave	2	manque d'attention
R19. Erreur de manipulation	Peu grave	2	manque d'attention
R20. Erreur de programmation	Grave	4	défaillance du dispositif de sécurité
R21. Perte de données	Très grave	5	défaillance du dispositif de sécurité
R22. Désastre environnemental	Très grave	5	Absence de contrôle
R23. Panne matérielle	Peu grave	2	Absence de contrôle
R24. Interruption du logiciel	Moyennement grave	3	défaillance du dispositif de sécurité
R25. Arrêt de l'activité	Très grave	5	défaillance du dispositif de sécurité
R26. Reprise d'activité compromise	Très grave	5	défaillance du dispositif de sécurité

Source : Nous-mêmes

Les cotations retenues ici tiennent compte des impacts présentés dans le tableau des risques et des critères de gravité définis plus haut.

6.2.3 Evaluation selon la criticité des risques identifiés

L'équation que nous utiliserons pour évaluer la criticité est la suivante :

Criticité= probabilité * gravité

Cette équation est la plus couramment utilisée et joue un rôle fondamental dans l'évaluation des risques.

La criticité déterminera le degré d'importance des risques de la SONABEL. Comme nous avons cinq (5) de probabilité et de gravité, la criticité minimale sera de 1 (1×1) et la criticité maximale sera de 25 (5×5).

Tableau 9: Evaluation de la criticité

Risques	Probabilité	Gravité	Criticité
R1. Accès non autorisé aux locaux informatiques	5	5	25
R2. Vol du matériel informatique	4	4	16
R3. Incendie	1	5	5
R4. Incidents électriques	3	3	9
R5. Coupure d'électricité	2	3	6
R6. Inondations	2	5	10
R7. Poussière	2	2	4
R8. Chaleur / Humidité	2	2	4
R9. Exposition aux attaques de virus	3	3	9
R10. Accès non autorisé au réseau	1	5	5
R11. Attaques des cybers pirates	1	5	5
R12. Vol de mot de passe	4	4	16
R13. Divulgations d'informations confidentielles	2	5	10
R14. Accès non autorisé au logiciel	3	5	15
R15. Saisie faussée de données	4	4	16
R16. Faille de sécurité	1	4	4
R17. Contre-mesure inefficace	1	4	4
R18. Erreur dans l'entrée des données	2	2	4
R19. Erreur de manipulation	2	2	4
R20. Erreur de programmation	2	4	8
R21. Perte de données	2	5	10
R22. Désastre environnemental	1	5	5
R23. Panne matérielle	2	2	4
R24. Interruption du logiciel	2	3	6
R25. Arrêt de l'activité	2	5	10
R26. Reprise d'activité compromise	2	5	10

Source : Nous-mêmes

6.3 Hiérarchisation des risques identifiés

Nous classerons ici les risques par ordre décroissant selon la probabilité, la gravité et la criticité.

Tableau 10 : Hiérarchisation selon la probabilité

Risques	Niveau	Cote
R1. Accès non autorisé aux locaux informatiques	Très forte	5
R2. Vol du matériel informatique	Forte	4
R12. Vol de mot de passe	Moyen	4
R15. Saisie faussée de données	Moyen	4
R4. Incidents électriques	Moyen	3
R9. Exposition aux attaques de virus	Moyen	3
R14. Accès non autorisé au logiciel	Moyen	3
R5. Coupure d'électricité	Faible	2
R6. Inondations	Faible	2
R7. Poussière	Faible	2
R8. Chaleur / Humidité	Faible	2
R13. Divulgations d'informations confidentielles	Faible	2
R18. Erreur dans l'entrée des données	Faible	2
R19. Erreur de manipulation	Faible	2
R20. Erreur de programmation	Faible	2
R21. Perte de données	Faible	2
R23. Panne matérielle	Faible	2
R24. Interruption du logiciel	Faible	2
R25. Arrêt de l'activité	Faible	2
R26. Reprise d'activité compromise	Faible	2
R3. Incendie	Faible	1
R10. Accès non autorisé au réseau	Très faible	1
R11. Attaques des cybers pirates	Très faible	1
R16. Faille de sécurité	Très faible	1
R17. Contre-mesure inefficace	Très faible	1
R22. Désastre environnemental	Très faible	1

Source : Nous-mêmes

Tableau 11: Hiérarchisation selon la gravité

Risques	Niveau	Cote
R1. Accès non autorisé aux locaux informatiques	Très grave	5
R3. Incendie	Très grave	5
R6. Inondations	Très grave	5
R10. Accès non autorisé au réseau	Très grave	5
R11. Attaque des cybers pirates	Très grave	5
R14. Accès non autorisé au logiciel	Très grave	5
R21. Perte de données	Très grave	5
R22. Désastre environnemental	Très grave	5
R25. Arrêt de l'activité	Très grave	5
R26. Reprise d'activité compromise	Très grave	5
R13. Divulgations d'informations confidentielles	Grave	5
R2. Vol du matériel informatique	Grave	4
R12. Vol de mot de passe	Grave	4
R15. Saisie faussée de données	Grave	4
R16. Faille de sécurité	Grave	4
R17. Contre-mesure inefficace	Grave	4
R20. Erreur de programmation	Grave	4
R4. Incidents électriques	Moyennement grave	3
R5. Coupure d'électricité	Moyennement grave	3
R9. Exposition aux attaques de virus	Moyennement grave	3
R24. Interruption du logiciel	Moyennement grave	3
R7. Poussière	Peu grave	2
R8. Chaleur / Humidité	Moyennement grave	2
R18. Erreur dans l'entrée des données	Peu grave	2
R19. Erreur de manipulation	Peu grave	2
R23. Panne matérielle	Peu grave	2

Source : Nous-mêmes

Tableau 12 : Hiérarchisation selon la criticité

Risques	Probabilité	Gravité	Criticité
R1. Accès non autorisé aux locaux informatiques	5	5	25
R2. Vol du matériel informatique	4	4	16
R12. Vol de mot de passe	4	4	16
R15. Saisie faussée de données	4	4	16
R14. Accès non autorisé au logiciel	3	5	15
R6. Inondations	2	5	10
R13. Divulgations d'informations confidentielles	2	5	10
R21. Perte de données	2	5	10
R25. Arrêt de l'activité	2	5	10
R26. Reprise d'activité compromise	2	5	10
R4. Incidents électriques	3	3	9
R9. Exposition aux attaques de virus	3	3	9
R20. Erreur de programmation	2	4	8
R5. Coupure d'électricité	2	3	6
R24. Interruption du logiciel	2	3	6
R3. Incendie	1	5	5
R10. Accès non autorisé au réseau	1	5	5
R11. Attaques des cybers pirates	1	5	5
R22. Désastre environnemental	1	5	5
R7. Poussière	2	2	4
R8. Chaleur / Humidité	2	2	4
R16. Faille de sécurité	1	4	4
R17. Contre-mesure inefficace	1	4	4
R18. Erreur dans l'entrée des données	2	2	4
R19. Erreur de manipulation	2	2	4
R23. Panne matérielle	2	2	4

Source : Nous-mêmes

- Les risques ayant une occurrence et un impact faible sont négligeables ;
- les risques ayant une forte occurrence et un impact important ne doivent pas exister, autrement une remise en cause des activités de l'entreprise est nécessaire (on évite le risque) ;
- les risques ayant une occurrence forte et un impact faible peuvent être acceptés ; leur coût est généralement inclus dans les coûts opérationnels de l'organisation (acceptation du risque) ;
- les risques ayant une occurrence faible et un impact lourd doivent être transférés. Ils peuvent être couverts par une assurance ou un tiers (transfert du risque) ;

- enfin, les autres risques, en général majoritaires, sont traités au cas par cas et sont au centre du processus de gestion des risques.

6.4 Recommandations

Elles sont formulées à partir des dispositifs de sécurité non existants relevés dans le tableau d'identification des risques.

6.4.1 Recommandations relatives à la sécurité physique

Au cours de notre stage, en observant les entrées et les sorties, nous avons remarqué que la porte accédant aux salles informatiques est parfois rabattue et certaines personnes y rentrent sans avoir accès. Ceci est dû au fait que certains agents entrent par badge en laissant la porte rabattue ou légèrement fermée derrières eux. Nous suggérons que la SONABEL mette en place un système de détection des personnes entrant dans les locaux informatiques sans badges ou empreintes comme par exemple les vidéos surveillances.
Aussi les locaux informatiques sont situés au rez-de- chaussée, ils ne sont donc pas protégés contre les dégâts des eaux en cas d'inondation.

6.4.2 Recommandations relatives à la sécurité des réseaux

A ce niveau, nous préconisons la mise en place de points de filtrage qui permet de lister tous les postes connectés pour renforcer la sécurité. Ceci dans le but de détecter toute tentative d'accès et de la bloquer avant qu'elle ne cause des dégâts.

6.4.3 Recommandations relatives aux mots de passe

Nous recommandons que la SONABEL de mettre en place un système efficace de gestion de ces mots de passe qui peut se faire par une simple configuration. A défaut, la SONABEL pourrait sensibiliser les utilisateurs à choisir des mots de passe robuste et veiller à les changer régulièrement. Elle pourrait aussi mettre en place un système pour prévenir l'usager des connexions précédentes sur son compte en affichant la date et l'heure (par exemple du dernier).

6.4.4 Recommandations relatives à la prévention, la détection et la neutralisation des logiciels malveillants

Pour y remédier, la SONABEL devrait renouveler les licences des antivirus et limiter les téléchargements à travers internet par les utilisateurs.

6.4.5 Recommandations relatives à la sauvegarde et le stockage des données

Nous proposons à la SONABEL pour éviter d'éventuels cas de perte de données, d'effectuer des tests de restauration occasionnels pour s'assurer de la fiabilité du système de sauvegarde. En plus de cela, la SONABEL devrait prévoir aussi un stockage de ses données hors site et mettre en place des procédures de reprise sur ce site extérieur régulièrement testé.
Le site extérieur peut par exemple être une sauvegarde en ligne. Celle –ci présente l'avantage d'externaliser de manière automatique la sauvegarde des données, qui seront sécurisées dans deux datacenters redondants et géographiquement distincts, l'accès aux données pour la récupération se faisant à travers un simple navigateur web.
Une procédure formalisée de l'archivage des données devrait être également prévue.

6.4.6 Recommandations relatives à la continuité des activités

Nous préconisons toujours pour assurer la continuité des activités, une politique de sauvegarde hors site des informations.

Conclusion :

Dans ce chapitre, nous avons pu identifier et évaluer les risques qu'encourt la SONABEL et par ordre d'importance. Il est donc important de prendre des mesures pour minimiser ceux qui ont un impact majeur. Les recommandations pourraient permettre à la SONABEL d'améliorer sa sécurité.

CONCLUSION DE LA DEUXIEME PARTIE

A l'issue de cette deuxième partie, nous pouvons dire qu'elle nous a permis de présenter la SONABEL et de prendre connaissance des mesures de sécurité appliquées et des dispositifs existants à travers les entretiens avec certains agents et aux documents auxquels nous avons eu accès. Elle nous a aussi permis de mettre en pratique notre modèle d'analyse et d'aboutir à l'évaluation des risques liés au logiciel Oracle.

Nos recommandations pourraient permettre de corriger certaines défaillances et améliorer la maîtrise des risques au sein de la SONABEL.

CONCLUSION GENERALE

L'environnement dans lequel évoluent les entreprises et les organisations est en proie aux crises ponctuelles et structurelles. L'entreprise est donc perpétuellement exposée à des divers risques.

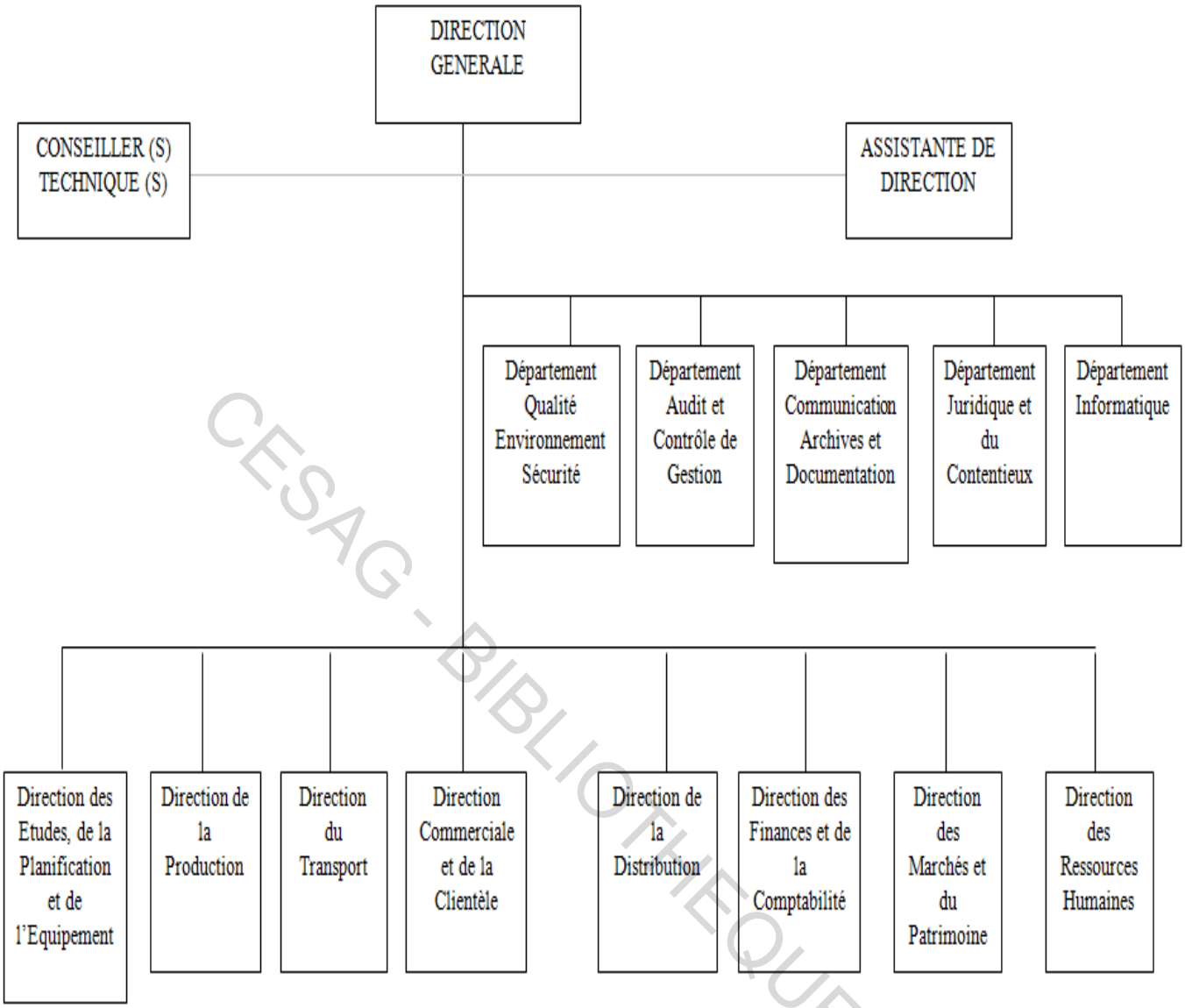
La problématique soulevée par ce document montre la nécessité de la prise en considération du risque informatique. Le risque est une notion à ne surtout pas négliger. Les paramètres à prendre en compte pour l'analyse des risques sont la fiabilité, la sécurité, la disponibilité. Nous avons également constaté que la divulgation d'informations joue un rôle important et qu'il devient nécessaire de sensibiliser de plus en plus le personnel de l'entreprise contre ce type de négligences coupables. Il est alors important de se doter de moyens techniques efficients pour rendre difficile les attaques externes au système d'information. Cette mise en œuvre a un coût financier non négligeable qu'il faut prendre en compte dès le départ lors de la mise en place de tout plan de sécurité

L'objectif de notre étude était d'évaluer liés les risques liés à la sécurité informatique, essentiellement du logiciel Oracle. Notre première partie a présenté les étapes de l'évaluation des risques tandis que la deuxième partie a consisté à appliquer la démarche à la SONABEL. Nous estimons au terme de notre étude que nos objectifs ont été atteints.

L'évaluation des risques est une étape centrale du management des risques. Le résultat de ce travail pourrait donc déterminer les grandes orientations du management des risques. Il revient alors à la SONABEL de s'approprier des méthodes et moyens nécessaires pour assurer leur maîtrise.

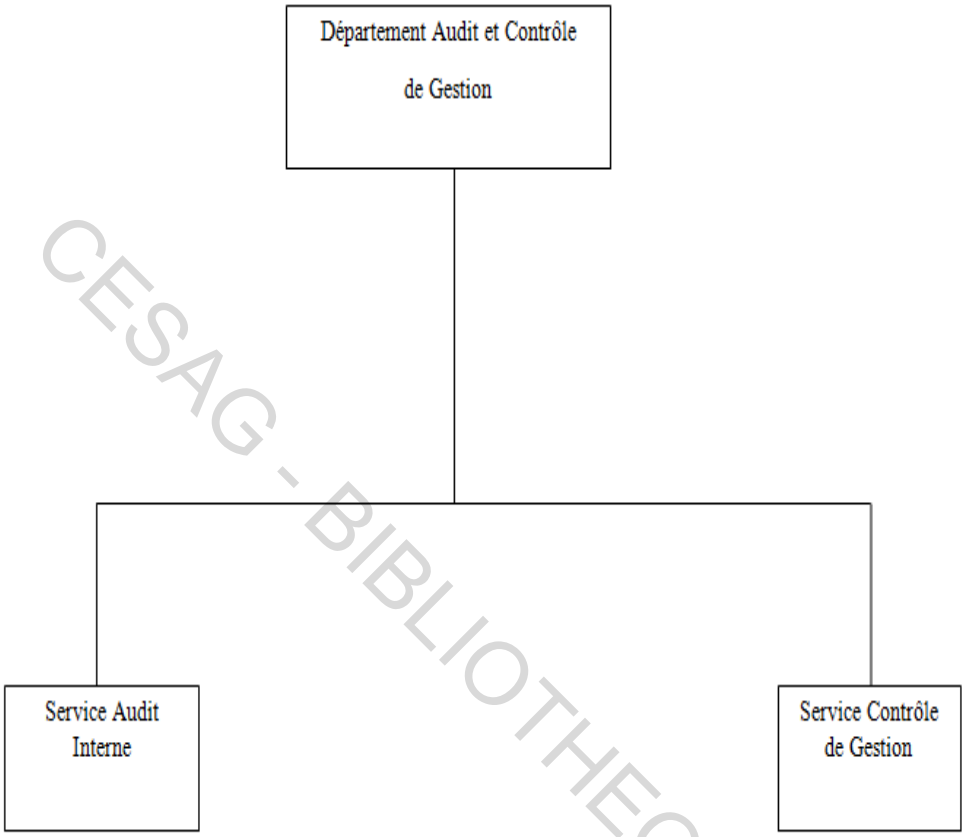
ANNEXES

Annexe 1 : Organigramme de la SONABEL



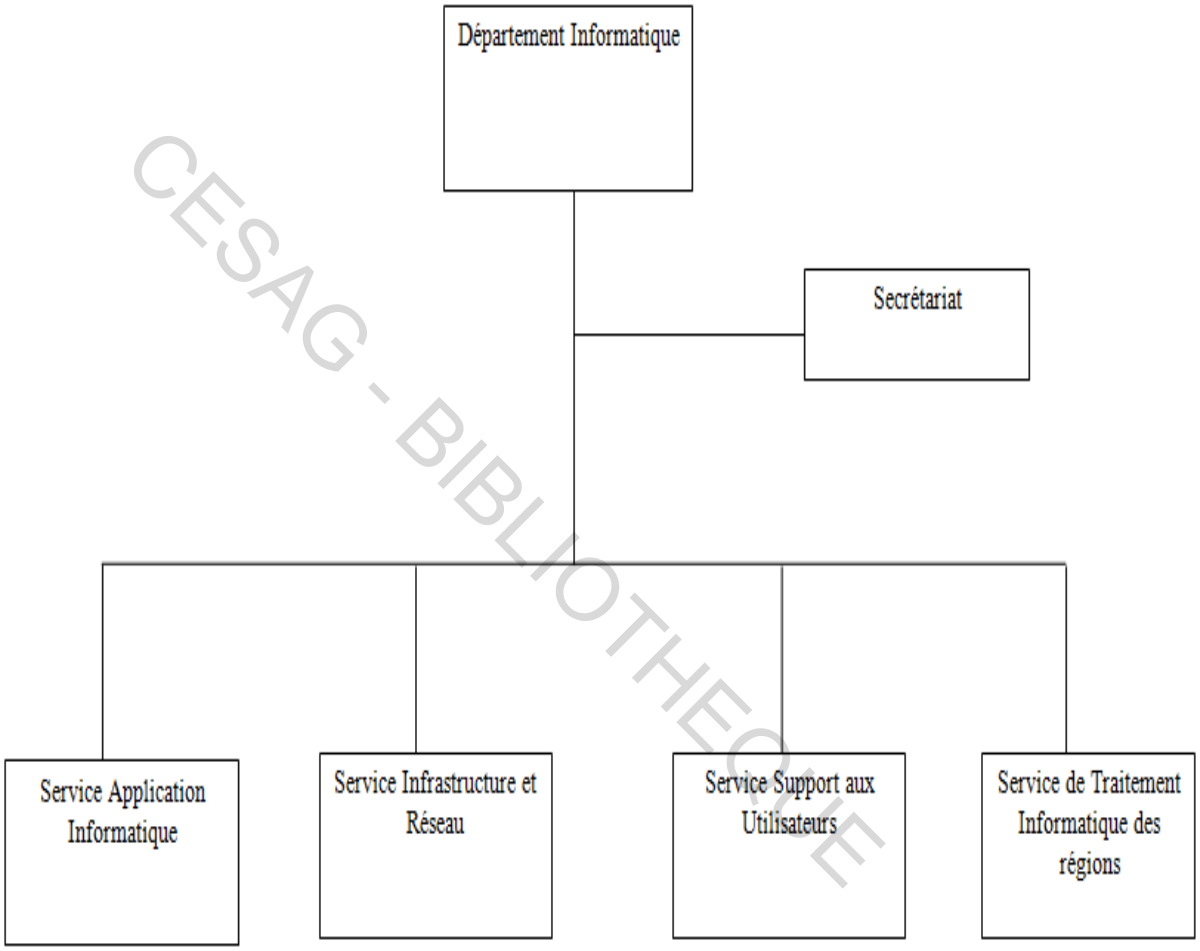
Source : Nous-mêmes, à partir du document relecture de l'organigramme de la SONABEL (2012)

Annexe 2 : Organigramme du département audit



Source : Document, relecture de l'organigramme de la SONABEL (2012)

Annexe 3 : Organigramme du département informatique



Source : Document, relecture de l'organigramme de la SONABEL (2012)

Annexe 4 : Questionnaire sur la sécurité physique

1- Comment accéder aux locaux informatiques ?
2- Existe-t-il un système de détection d'intrusion des personnes non autorisées
3- Existe-t-il dispositif de détection et d'extinction automatique d'incendie ?
4- Quelles sont les dispositions prises pour la protection électrique ? (panne et incidents électriques)
5- Est-ce que l'entreprise dispose d'onduleurs qui assurent la disponibilité et la continuité des activités ?
6- La climatisation dans la salle serveur est-elle adéquate ?
7- La salle informatique est-elle située en hauteur ?
8- Quelles sont les mesures permettant de sécuriser le matériel informatique ?
9- Existe-t-il des contrats d'assurance du matériel ?
10- Quel est le plan de secours informatique ainsi que celui de la continuité des activités ?
11- Est-ce que l'entreprise dispose d'une charte informatique ?

Annexe 5 : Questionnaire sur la sécurité du réseau

1- Qui peut accéder au réseau ?
2- Cet accès est-il règlementé ?
3- Toute intrusion est-elle détectée immédiatement ?
4- Quelles sont les dispositions mises en place pour protéger le réseau ?
5- Quelles sont les dispositions mises en place pour identifier les risques et les menaces potentiels vis-à-vis du réseau ?

Annexe 6 : Questionnaire sur le logiciel Oracle

1- Existe-t-il des mots de passe ?
2- Si oui sont –ils affectés individuellement à chaque utilisateur ?
3- Les mots de passe sont-ils changés régulièrement ?
4- Si oui à quelle fréquence ?
5- Existe-t-il un gestionnaire des mots de passe ?
6- Quel est le nombre de licence ?
7- Quel est le nombre des utilisateurs ?
8- L'accès au logiciel est-il contrôlé et règlementé ?
9- Comment est fait le paramétrage du logiciel ?
10- Est-il possible de détecter les tentatives d'accès non autorisés ?
11- En cas d'interruption du logiciel comment récupérer les données ?
12- Existe-t-il une procédure de sauvegarde clairement définie ?
13- Le système de sauvegarde des données est-il fiable ?
14- Y'a-t-il déjà eu des cas de pertes de données ?
15- Existe-t-il des sauvegardes hors site ?
16- Comment se fait l'archivage des données ?
17- Existe-t-il des antivirus ?
18- Sont-ils mis à jour régulièrement ?
19- En cas de démission, de licenciement ou de congé d'un utilisateur existe-t-il un système de suppression des mots de passe ?
20- Quelle est la procédure de validation des opérations comptables ?
21- Est-ce possible de modifier ou supprimer après la validation ?
22- Quel est le degré de fiabilité du logiciel ?
23- Existe-t-il une documentation du logiciel permettant son utilisation adéquate ?
24- Quels sont les risques déjà survenus ?
25- Le personnel est- il informé sur les risques encourus par l'utilisation du logiciel ?

Annexe 7 : Exemple de FRAP (Feuille de Révélation et d'Analyse de Problème)

Feuille de Révélation et d'Analyse de Problèmes
Papier de travail **FRAP N°**
Risque identifié : risque d'accès non autorisé aux locaux informatiques
Constats : ➢ La porte accédant aux locaux informatiques est fréquemment rabattue et non totalement fermée
Causes explicatives : ➢ Défaillance du système de sécurité ➢ Absence de contrôle des accès
Conséquences : ➢ Vol du matériel informatique ➢ Destruction des actifs informatiques
Recommandations : ➢ Mettre en place un système de détection d'intrusion (vidéo surveillance par exemple) ➢ Mettre en place un système de gardiennage
Etabli par: Nous-mêmes **Approuvé par : Le responsable informatique**

Source : Nous-mêmes

BIBLIOGRAPHIE

1- BARTHELEMY Bernard, COURREGES Philippe (2004), *gestion des risques*, 2e édition, Editions d'organisation, 472 pages ;

2- Christian Jimenez, Patrick Merlier, Dan Chelly (2008), *Risques opérationnels : de la mise en place du dispositif à son audit,* Revue banque édition, 271 pages ;

3- COSO II (2005), *le management des risques de l'entreprise : cadre de référence, techniques d'application,* Edition d'Organisation, paris, 337pages ;

4- CURABA Sandra, JARLAUD Yannick, CURABA Salvatore (2009), *Evaluation des risques : comment élaborer un document unique,* Edition Afnor, 325 pages ;

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

6- DESMOULINS Nicolas (2009), *maîtriser le levier informatique : accroître la valeur ajoutée des systèmes d'informations,* Pearson, Paris, 286 pages ;

7- DESROCHES Alain, LEROY Alain, VALLEE Frédéric (2003), la gestion des risques, principes et pratiques, 286 P ;

8- IFACI (2009) ; Normes, The Institut of Internal Auditors, Paris, 66 pages ;

9- IFACI, PRICEWATERHOUSECOOPERS et al. (2005), *le management des risques de l'entreprise : cadre de référence- Techniques d'application,* Les Editions d'Organisation, Paris, 338 pages ;

10- LAFITE Michel (2003) ; *sécurité des systèmes d'information et maitrise des risques*, Edition REVUE BANQUE, Paris, 210 pages ;

11- Laurent Bloch, Cristophe Wolfhugel (2007), *sécurité informatique, principes et méthodes*, éditions EYROLLES, Paris, 261 pages ;

12- Le petit larousse 2010, 1883 pages ;

13- LY, Henri (2005), *L'audit technique informatique,* Editions LAVOISIER/HERMES SCIENCE, Paris, 230 pages ;

14- RENARD Jacques (2004), *Théorie et pratique de l'audit interne*, 4eme édition, édition d'organisation, 462 pages ;

15- RENARD Jacques (2009), *Théorie et pratique de l'audit interne,* 463 pages ;

16- RENARD Jacques (2010), *théorie et pratique de l'Audit Interne, 7eme édition, édition d'organisation*, Groupe Eyrolles, Paris, 469p ;

17- ROUFF Jean Loup (2001), *Des concepts et des mots*, Revue Audit n° 153 : 12-27, Paris ;

18- SHICK Pierre (2007), Mémento d'audit interne, *Méthode de conduite d'une mission*, DUNOD, Paris, 217 pages ;

19- SHICK Pierre et al. (2010), *audit interne et référentiel des risques*, DUNOD, Paris, 340 pages ;
20- VOLLE, Michel (2004), *Lexique du système d'information*, club des maîtres d'ouvrages des systèmes d'informations & Michel VOLLE, GNU Free Documentation, Paris, 23 pages.

Articles :

21- ISO/IEC 17799 :2005 la sécurité de l'information, *Code de pratique pour la gestion de sécurité d'information* Vol.1(2) :115.
22- SONABEL, 2012, Relecture de l'organigramme, *description de missions des structures*, Vol.2 (3) : 66.

Sources internet :

23- La SSI pour les nuls (2013), les domaines de la SSI/la sécurité physique et environnementale, http://www.lassipourlesnuls.fr/la-ssi/les-domaines-de-la-ssi/securite-physique-et-environnementale/;
24- Scribd (2013), Les outils après le travail de terrain, http://fr.scribd.com/doc/61356616/FRAP;
25- Net Gestion (2014), les risques informatiques, http://www.net-gestion.fr/PBCPPlayer.asp?ID=1385774;
26- Comment ça marche.net (2014), protection introduction a la sécurité des réseaux, http://www.commentcamarche.net/contents/995-protection-introduction-a-la-securite-des-reseaux ;
27- 01net (2013), protéger ses infrastructures : la sécurité physique requiert des spécialistes, http://www.01net.com/editorial/175234/3-proteger-ses-infrastructures-la-securite-physique-requiert-des-specialistes/;

28- Eduscol (2013), sécurité des systèmes d'informations: de la gestion des risques à la confiance numérique, http://eduscol.education.fr/ecogest/si/SSI/risk_conf;
29- Cisco.com (2013), tout ce que vous devez savoir sur la sécurité des réseaux, http://www.cisco.com/web/FR/solutions/smb/products/security/security_primer.html#1;
30- Le monde informatique (2013), actualité micro, http://www.lemondeinformatique.fr/;

31- Le monde informatique (2013), harward et matériel informatique, http://www.lemondeinformatique.fr/hardware-et-materiel-informatique-9.html;

32- Sonabel.bf (2014), actu news, www.sonabel.bf;

33- Wikipedia (2013), Wikimedia France, www.wikipédia.fr.