CESAG

Centre Africain d'études Supérieures en Gestion

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

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

Promotion 22
(2010-2011)

Mémoire de fin d'étude
THEME

EVALUATION DES RISQUES LIES AUX APPLICATIONS INFORMATIQUES DE LA SOCIETE COTONNIERE DU TCHAD «COTONTCHAD»

Présenté par:
M. Djikolmbaye DJEGOL

Dirigé par:
M. Alain SAWADOGO
Professeur Associé au CESAG

Avril 2012

DEDICACES

A mes enfants, ALLARAMADJI D. Cédric et REMADJI D. Régine.

A mon épouse MBAIAMDENE Grâce.

A mes parents, mes frères et sœurs.

REMERCIEMENTS

Je souhaite témoigner toute ma profonde gratitude et mes remerciements les plus sincères à **Monsieur MAHAMAT ADOUM Ismaël,** Président-Directeur Général de la COTONTCHAD, pour m'avoir permis d'accéder à cette formation qui est pour moi le plus important de mes projets professionnels.

J'exprime également ma profonde gratitude et mes remerciements sincères à mon Directeur de Mémoire (DM) **Monsieur SAWADOGO Alain** pour ses conseils et le temps qu'il m'a accordé pour la réalisation de ce rapport.

Je remercie, au même titre, **Monsieur Moussa YAZI**, Directeur de l'ISCBF du CESAG, qui veille continuellement à la qualité de la formation assurée au sein de cet Institut. Je remercie, bien sûr, le corps professoral et le personnel administratif du CESAG pour leurs conseils et orientations durant notre séjour dans cette institution.

Je tiens à remercier tout particulièrement:

- **M. AHMED DJONOUMA DJASRABE,** Chef de Département Informatique pour sa participation à notre étude et son soutien durant notre "passage" dans cette entité.
- **M. NODJIHOREM Béral**, Directeur Administratif et des Ressources Humaines et tous ses collaborateurs;
- **M. NDERNGUE Guidmingar**, Directeur du Contrôle de Gestion et Audit Interne et les collègues auditeurs internes et contrôleurs de gestion, en particulier:
  - **M. MAYO MADJIASSEM**, Chef de Service Contrôle de Gestion;
  - **M. MBAINAISSEM Elisée**, contrôleur de gestion;
  - **M. MOSSE TORMBAYE**, Auditeur interne;
  - **M. TEIBETCHANG Justin**, Auditeur interne;
  - **M. TCHANA Pelguem**, Auditeur interne.
- M. **ALLAOUTENGAR MANDIGUI**, Directeur Financier et Comptable et ses collaborateurs pour les échanges constructifs et fructueux que nous avons eu avec eux.

Je tiens à remercier, enfin, **Monsieur MABAINAISSEM TEDJI**, Ex-Directeur Général de la COTONTCHAD, pour tous ses conseils, son soutien et ses encouragements.

LISTE DES TABLEAUX ET FIGURES

Liste des tableaux

Liste des figures

LISTE DES SIGLES ET ABREVIATIONS

AFAI:	Association Française de l'Audit et du Conseil Informatiques
AMF:	Autorité des Marchés Financiers
CIGREF:	Club Informatique des Grandes Entreprises Françaises
CLUSIB:	Club de Sécurité Informatique Belge
CLUSIF:	Club de la Sécurité de l'Information Français
COBIT:	Control Objectives for Information and related Technology
COCO:	Criteria Of COntrol
COSO:	Committee Of Sponsoring Organizations of the Treadway Commission
DSI:	Direction des Systèmes d'Information
EBIOS:	Expression des Besoins et Identifications des Objectifs de Sécurité
EDI:	Echange de Données Informatisées
IBM:	International Business Machine
IFACI:	Institut Français de l'Audit et du Contrôle Internes
ISO:	International Organisation for Standardization
MARION:	Méthodologie d'Analyse des Risques Informatiques Orientée par Niveau
MEHARI:	Méthode Harmonisée d'Analyse des Risques
PC:	Personnal Computer
PDG:	Président-Directeur Général
SGSI:	Système de Gestion de la Sécurité de l'Information
SLA:	Service Level Agreement
SN:	Société Nouvelle

LISTE DES ANNEXES

TABLE DES MATIERES

INTRODUCTION GENERALE

Le risque fait partie intégrante des activités de l'entreprise, et sur un marché dynamique et désormais mondialisé, où règnent le changement et les incertitudes, il connait un développement spectaculaire. Un risque peut être associé à toute activité, à toute décision, à toute action. Les acquisitions d'entreprises, les partenariats basés sur la collaboration, l'intégration mondiale et les évolutions technologiques incessantes sont autant des facteurs de risque. Aujourd'hui, les entreprises les plus performantes ont parfaitement compris comment les absorber et les limiter au mieux.

Aussi, dans un environnement marqué par l'omniprésence de l'informatique au cœur de toutes les activités de l'entreprise, la capacité d'adaptation repose essentiellement sur l'aptitude à gérer efficacement les risques auxquels sont exposés l'informatique, l'infrastructure physique et les processus métier de l'entreprise.

Les risques informatiques peuvent être désignés comme les risques « métiers » associés à l'utilisation, la possession, l'exploitation, l'implication, l'influence et l'adoption de l'outil informatique dans une organisation. On assiste de nos jours à une prise en considération croissante des besoins de maîtrise des risques informatiques opérationnels du fait même de l'usage extensif des nouvelles technologies, de l'existence d'une infrastructure informationnelle globale et de l'émergence de nouveaux risques.

Les systèmes informatiques mis en réseau sont des ressources accessibles à distance et deviennent des cibles potentielles d'attaques informatiques. Cela accroit les risques d'intrusions des systèmes et offre un terrain favorable à la réalisation, à la propagation des attaques et des délits. Les attaques portent atteintes à la capacité à traiter, sauvegarder, communiquer le capital informationnel, aux valeurs immatérielles, aux processus de production ou de décision de ceux qui les possèdent. Les systèmes informatiques introduisent de ce fait des risques opérationnels dans le fonctionnement des organisations qui les possèdent.

Pour ce faire, l'identification et l'évaluation des risques opérationnels informatiques ou de leurs facteurs, plus qu'une nécessité, est une des préoccupations majeures de tout responsable d'une entreprise et devient dès lors une véritable exigence du responsable informatique qu'il partage avec ses homologues opérationnels des lignes métiers.

L'acquisition de nouvelles applications par la COTONTCHAD, la mise en réseau de son dispositif informatique connecté à l'internet, l'insuffisance du personnel qualifié, le manque de formation ou l'insuffisance de budget conséquent accroissent la probabilité que les risques inhérents ou liés à l'informatique se matérialisent. De plus les locaux abritant les infrastructures informatiques peuvent être la cible d'individus ou d'organisations malveillants ou faire l'objet d'incendie pouvant compromettre la disponibilité, l'intégrité, la confidentialité.... et mettre en péril la continuité de l'exploitation ou la bonne conduite des missions assignées à la société.

L'absence de maîtrise des risques et/ou l'atteinte à la sécurité du dispositif informatique peut conduire à l'interruption des activités de la société en raison:

- d'une indisponibilité du système informatique causée par les faits suivants:
  - panne d'un composant du réseau (par exemple routeur);
  - incendie de la salle machine ;
  - intrusion d'un pirate et destruction des bases des données;
  - plan de secours inexistant ou mis à jour ou encore n'ayant pas suivi l'évolution récente des systèmes et applications.
- d'une fraude causée par:
  - accès inappropriés aux données: possibilités d'intervention directe sur les fichiers d'interface, sans supervision;
  - absence de contrôle au sein des processus;
  - anomalies de séparation de tâches au sein de la communauté d'utilisateurs;
  - absence d'outil de détection d'anomalies en place sur les données;

D'une façon générale, les risques informatiques ont pour origine dans:

- *les causes accidentelles*: choc, coupure des câbles électriques, incendie, foudre, inondation, tempête, dégâts des eaux, ... pannes, dysfonctionnement ou défaillance de matériel ou de logiciel de base, d'origine interne ou externe;
- *les erreurs*: erreurs de saisie, de transmission et d'utilisation de l'information; erreurs d'exploitation; erreurs de conception et de réalisation;
- *la malveillance*: vol et sabotage du matériel; sabotage immatériel; fraude; indiscrétion et détournement d'informations; détournement de logiciels;
- *grève ou départ de personnel stratégique*.

Les conséquences des tels risques informatiques, qu'elles soient directes ou indirectes, sont nombreuses et peuvent entraîner des dommages considérables:

- destruction totale ou partielle de plusieurs composants d'un système d'information à savoir, matériel informatique ou de communication, supports de données, locaux.
- indisponibilité du système d'information pouvant provoquer l'arrêt des activités de l'entreprise; impossibilité d'accéder au réseau internet; pertes des marchés;
- pertes, altérations ou détournements des logiciels ou données et transmissions des mauvais fichiers;
- litiges pouvant entrainer des paiement des dommages et intérêts importants;
- frais de reconstitution des données et d'archives, frais d'études et d'expertises;
- pertes d'exploitation.

Au regard de ce qui précède, des mesures doivent être envisagées pour absorber et limiter au mieux les risques opérationnels, notamment informatiques, objet de notre étude. Il s'agit entre autres de:

- sensibiliser le personnel et les autres acteurs aux problèmes de sécurité;
- mettre en place une politique de sécurité adaptée au contexte de la société COTONTCHAD;
- recruter un personnel complémentaire qualifié et compétent et établir un plan de relève du personnel stratégique;
- créer un poste de responsable de sécurité informatique;
- nommer, si possible, un Risk Manager (RM);
- procéder à des audits de sécurité des systèmes et applications informatiques;
- élaborer une cartographie des risques régulièrement mise à jour et envisager des mesures pour traiter les risques résiduels, à savoir:
  - accepter les risques résiduels (acceptation);
  - éliminer, si possible, les risques résiduels (élimination);
  - limiter l'amplitude ou transférer les risques résiduels (protection);
  - réduire la probabilité de survenance des risques résiduels (prévention).

La dernière solution relative à l'élaboration d'une cartographie des risques nous semble judicieuse pour être retenue.

La question principale est celle de savoir comment évaluer les risques opérationnels inhérents ou liés aux applications informatiques et par conséquent ceux des infrastructures informatiques sans lesquelles les applications ne fonctionneraient pas?

De façon spécifique:

- comment identifier les risques informatiques inhérents?
- quels sont les éléments permettant de quantifier les risques informatiques?
- quelle est la méthode d'évaluation des risques opérationnels liés aux applications informatiques?
- quelles données recueillir pour aboutir à une cartographie des risques informatiques?
- quels sont les facteurs de risques liés aux applications?

C'est à ces différentes questions que nous tenterons d'y apporter des réponses au travers de notre étude portant sur le thème: **Evaluation des risques opérationnels liés aux applications informatiques de la société cotonnière du Tchad, « COTONTCHAD».**

L'objectif général de l'étude consiste à évaluer les risques opérationnels des applications informatiques. De façon plus spécifique, il s'agit de:

- identifier les risques opérationnels encourus au sein des applications informatiques;
- préciser les critères de cotation des risques informatiques;
- identifier les menaces liées aux applications informatiques;
- identifier les vulnérabilités liées aux applications informatiques;
- étudier les contremesures ou dispositifs de sécurité à mettre en place pour réduire les risques informatiques;
- préciser les mesures de contrôles qui seront prises afin de réduire les risques;

L'évaluation des risques informatiques couvre des domaines plus larges. Cependant notre étude sera limitée à l'identification et l'évaluation des risques opérationnels liés aux processus et applications informatiques. Nous examinerons également les dispositifs de contrôle interne mis en œuvre pour protéger les données, infrastructures et applications contre les menaces internes ou externes afin de dégager les forces, les faiblesses et formuler des recommandations. Dans cette perspective, nous étudierons les procédures mises en place (si elles existent) ou susceptibles de l'être pour une reprise rapide des activités en cas de matérialisation de sinistre de grande amplitude.

L'intérêt d'une telle étude pour la société COTONTCHAD est évident dans la mesure où celle-ci peut en tirer des avantages multiples:

- des informations détaillées sur les menaces qui pèsent sur l'entreprise et qu'elle ne cernait pas distinctement;
- un inventaire des risques opérationnels formalisé et partagé permettant de lancer des actions ou projets ciblés pour les maitriser (par exemple, la cartographie des risques est une méthode répandue, mise en œuvre par de nombreuses entreprises);
- une appréciation de la sensibilité et de la responsabilisation des principaux managers face aux risques de l'entreprise.

In fine, l'intérêt d'une bonne politique de gestion des risques est:

- la réduction des pertes opérationnelles;
- la baisse des coûts des audits;
- la détection anticipée et plus rapide des risques;
- l'exposition réduite aux dangers;
- une meilleure diffusion de l'information;
- l'amélioration des performances des activités.

Pour nous, en tant qu'auditeur interne de la COTONTCHAD, ce travail croise particulièrement notre centre d'intérêt dans la mesure où les résultats pourront être d'une grande utilité dans l'élaboration des plans d'audit interne: approche par les risques dans l'identification et l'évaluation de ces risques, élaboration et mise à jour de la cartographie des risques informatiques pour des missions d'audit interne.

Dans le même ordre d'idée, ce travail peut constituer pour l'audit interne un outil appréciable à l'audit des systèmes et/ou applications informatiques de la société COTONTCHAD. C'est enfin pour nous l'aboutissement de notre parcours de formation dont l'intérêt est de confronter les aspects théoriques aux réalités spécifiques de notre entreprise et d'en tirer les conclusions qui pourraient être certainement édifiantes.

Notre étude comportera deux parties décrites comme suit:

- **première partie: cadre théorique de l'étude.**

Il s'agit, dans cette partie, de faire une revue de la littérature sur le sujet. A cet effet, le premier chapitre traitera des risques opérationnels informatiques en général (environnement et

applications). Au deuxième chapitre, nous aborderons la démarche classique d'évaluation des risques mais également celle du contrôle interne destiné à couvrir ces risques. Le troisième et dernier chapitre de cette partie théorique sera consacré à l'approche méthodologique qui sera déroulé et mis en œuvre au cours de la phase pratique de l'étude.

- **deuxième partie: cadre pratique**

Le quatrième chapitre, début de cette partie, sera consacré à la présentation de la COTONTCHAD, structure sur laquelle est axée notre étude. Ensuite, une description du dispositif informatique et des applications existants sera traitée au cinquième chapitre. Enfin, l'évaluation, proprement dite, des risques liés aux applications informatiques fera l'objet du sixième et dernier chapitre.

PREMIERE PARTIE: CADRE THEORIQUE

INTRODUCTION DE LA PREMIERE PARTIE.

Toute organisation, quelque soit sa taille et le degré d'automatisation de son système d'information et ses processus, comporte des risques inhérents et/ou liés au fonctionnement de ces derniers. Les risques informatiques, comme tout risque opérationnel, constituent de nos jours une grande préoccupation pour tout chef d'entreprise, soucieux du bon fonctionnement et de la rentabilité de celle-ci.

Les risques informatiques ou risques « métiers » sont des risques opérationnels associés à la possession, l'utilisation, l'exploitation et l'adoption de l'outil informatique dans une organisation. La survenance de ces risques par rapport aux menaces encourues est susceptible de générer des conséquences très dommageables pour l'entreprise et la conduire, dès lors, à une situation pouvant compromettre sa continuité ou sa survie.

L'identification et l'évaluation de ces risques, suivants des méthodes et techniques de référence peut permettre à l'entreprise de prendre des mesures adéquates de protection, de prévention ou de réduction de ces dangers.

Cette partie de notre étude sera consacrée à une revue de la littérature sur les risques opérationnels informatiques, la démarche et les outils d'identification et d'évaluation des risques opérationnels liés aux applications informatiques ainsi que l'approche méthodologique de leur mise en œuvre.

CHAPITRE I: LES RISQUES OPERATIONNELS INFORMATIQUES

Introduction

Après avoir précisé le concept de risque, un bref aperçu du dispositif informatique couramment rencontré dans les organisations sera présenté. Les risques opérationnels seront abordés du point de vue informatique selon leurs origines ainsi que les dispositifs théoriques de maitrise de ces risques.

1.1. Définition et concept de risque.

Le concept de risque est difficile à cerner car ce dernier peut être considéré comme un évènement redouté dont la survenance, ne pouvant être connue avec certitude, est susceptible d'entrainer des pertes ou dommages. Le risque peut être défini comme suit:
«[Le risque est] la menace qu'un évènement, une action ou une inaction affecte la capacité de l'entreprise à atteindre ses objectifs stratégiques et compromettent la création de la valeur» (ERNST & YOUNG in MOREAU 2002: 3). Ce qui montre que l'occurrence d'un risque résulte de l'effet d'une menace sur une vulnérabilité.

Aussi, «Le risque est défini comme la mesure d'un ensemble d'éléments de la situation dangereuse qui, combinés à des conditions particulières d'environnement, redoutés ou non, connues ou non, peuvent entrainer des conséquences préjudiciables ou accidentelles.» (DESROCHES & AL, 2003: 33). En d'autres termes, le risque ne devient un danger réel, générant des dommages, que si certaines conditions spécifiques d'environnement sont réunies.

Selon SCHICKE & AL. (2010; 10), «Le RISQUE est un concept signifiant la possibilité que la combinaison d'un évènement incertain et d'un mode fonctionnement aléatoire ait pour conséquence la non atteinte d'un objectif.»

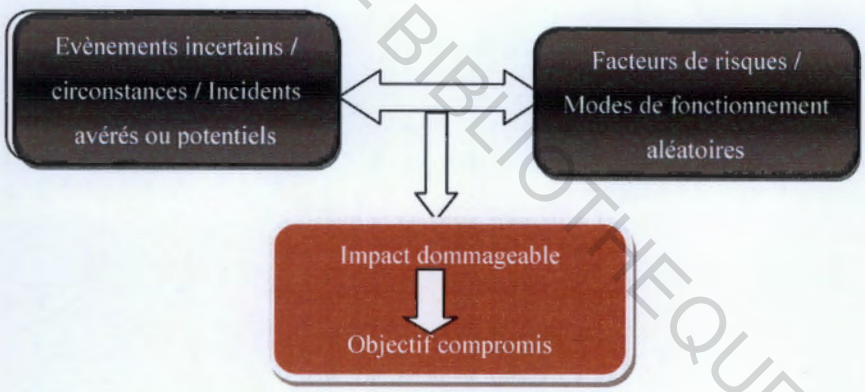
Ces définitions contribuent à nous faire percevoir que toute survenance d'un évènement ayant un impact négatif sur le bon fonctionnement d'une organisation constitue de ce fait un risque. L'intérêt de ces définitions est qu'elles soulignent, plus ou moins, que le

risque est lié d'une part à sa probabilité d'apparition et d'autre part à la gravité de ses conséquences sur les objectifs fixés. Un risque se caractérise donc par deux grandeurs à savoir une probabilité d'occurrence et la gravité des effets. De ce fait, il y a lieu de se rendre compte qu'il n'y a de risque que par rapport à l'atteinte d'un objectif ou plus précisément, par rapport à la conséquence dommageable subie (SCHICK, 2010).

En définitive, la manifestation d'un fait ou évènement incertain seul ne suffit pas à générer des impacts ou conséquences négatifs sur l'atteinte des objectifs, il faut en plus un élément déclencheur à savoir le facteur du risque, réputé en être la cause.

Nous pouvons résumer les différentes définitions conceptualisant la notion de risque par la figure suivante.

Figure 1: Le concept de risque



Source: Adaptée de SCHICK & AL. (2010; 11)

Selon SHICK & Al. (2010: 12), «les facteurs de risque qui, combinés à la survenance des évènements incertains, vont ou ne vont pas entrainer de conséquences dommageables, sont tous à rechercher dans l'organisation et le fonctionnement de l'entreprise ou l'entité concernée». Pour pallier ces risques, des mesures doivent êtres mises en œuvre dans le cadre du dispositif de contrôle interne de l'organisation.

Selon FABRE, SEPARI & Al. (2007: 50); les risques opérationnels sont «ceux liés à la gestion quotidienne principalement (pannes des machines, rupture de stock, dysfonction dans une ou plusieurs activités opérationnelles, défauts…).... Ces risques sont susceptibles

d'entraver la réalisation des objectifs à court terme et ils représentent des enjeux financiers et sans doute humains (risque d'accident…)».

Le comité de Bâle (Bâle II) définit le risque opérationnel comme suit: «Le risque opérationnel est le risque de pertes provenant de processus internes inadéquats ou défaillants, de personnes et systèmes ou faisant suite à des évènements externes». Il se dégage de cette définition quatre composantes considérées comme origines ou source des risques opérationnels à savoir :

- défaillances dues aux processus: erreurs de saisie, omissions, non-conformité règlementaire, processus lourds et inopérants, procédures et directives inefficaces ou non appliquées…;
- défaillances dues aux personnes: fraude, défaut de conseil, inadéquation de compétences, fautes intentionnelles, vol ou détournement d'actifs, conflits sociaux,…;
- défaillances dues aux systèmes d'information: indisponibilité des systèmes, pannes détérioration des données, défaillance liée au matériel, virus informatique, intrusion....;
- défaillances dues aux évènements extérieurs: incendie, inondation, évolution règlementaires fortes, litiges avec les parties prenantes, etc.

Ces définitions, montrent que les risques informatiques font partie intégrantes des risques opérationnels. Toute entreprise peut être concernée par ce type de risque. Mais avant d'aborder les risques informatiques, il convient de décrire succinctement le système informatique et les applications considérés, de nos jours, comme un support incontournable du système d'information de l'entreprise.

1.2. Le dispositif informatique: support du système d'information

Selon VOLLE (2004: 21), «le système informatique est l'ensemble des moyens matériels et logiciels assurant le stockage, le traitement et le transport des données sous forme électronique.». Il existe donc une relation étroite entre système informatique et système d'information en ce sens que le premier se trouve être le support par excellence du second.

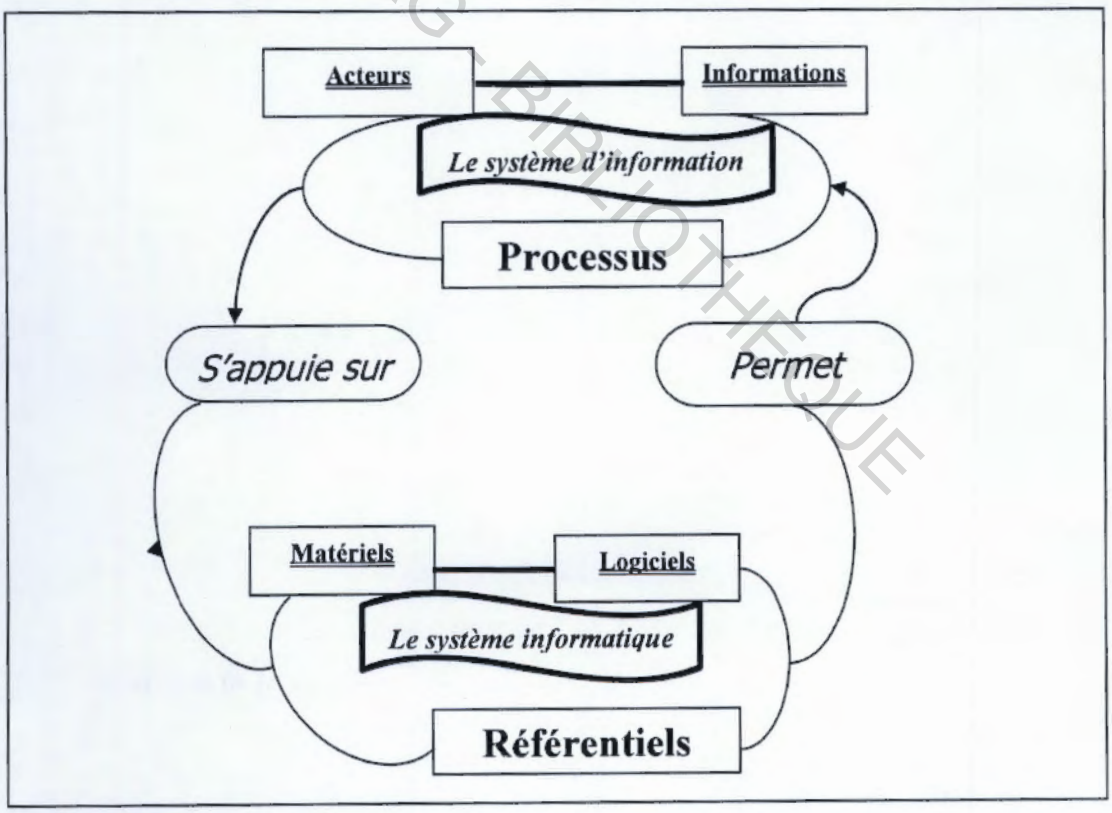
Pour DAYAN & AL. (2004: 1075), «le système informatique est le support technique du système d'information de l'entreprise. Cela regroupe les moyens informatiques (serveurs et postes utilisateurs) et les moyens de communication (réseaux)».

Nous pouvons donc affirmer que le système informatique est une composante essentielle du système d'information, pris dans sa globalité. A cet effet, il est le support par exeellence du système d'information qui, lui-même, fait partie intégrante de l'organisation.

Nous retenons, enfin, que le système informatique est constitué de postes de travail (micros ordinateurs), des supports de stoekage, des serveurs et des réseaux sans lesquels l'automatisation du système d'information ne fonctionnerait pas. On pourrait y ajouter, dans le même ordre d'idée, des applications métiers, des bases de données de l'entreprise et certainement les dispositifs de sécurité informatiques. Comme traduit sur la figure ci-dessous, le système informatique est le support sur lequel s'appuie le système d'information de l'entreprise.

Figure 2: Système d'information et système informatique

« Le système informatique est le support du système d'information ».



Source: Nous même, adapté de DESMOULINS (2009: 14).

1.2.1. Les serveurs

Selon YADAV & SINGH (2009), un serveur est à la fois un ensemble de logiciels et l'ordinateur les hébergeant, dont le rôle est de répondre de manière automatique à des demandes envoyées par des clients (ordinateur et logiciel) via le réseau. Les utilisations courantes des serveurs sont le serveur de fichiers, d'impression, de base de données, de courrier, ainsi que le serveur web, le serveur d'applications, le proxy et le serveur de jeux. Un proxy étant un service qui partitionne la communication entre le client et le serveur en établissant un premier circuit entre le client et le firewall (coupe-feu), et un deuxième entre ce dernier et le serveur (Internet).

Un serveur de fichiers est utilisé pour le stockage et le partage de fichiers entre plusieurs utilisateurs. Un serveur d'impression est utilisé comme intermédiaire entre un ensemble d'imprimantes, tandis qu'un serveur de base de données est utilisé pour stocker et manipuler des données contenues dans une ou plusieurs bases et partagées entre plusieurs utilisateurs.

Un serveur de courrier est utilisé pour stocker et transmettre du courrier électronique. Un serveur web stocke et manipule les pages d'un site web et les transmet sur demande de l'utilisateur. Un serveur de jeu arbitre et suit l'évolution d'un jeu en mettant en communication les différents joueurs.

Un serveur d'application effectue les traitements d'un ou plusieurs logiciels applicatifs à architecture Client/serveur. Un serveur proxy (mandataire) reçoit des demandes, les contrôle, puis les transmet à d'autres serveurs, (YADAV & SIGH, 2009).

En définitive, un serveur, au sens informatique, est un ordinateur et/ou un logiciel, dont le but est de rendre des services à d'autres ordinateurs ou logiciel connectés à l'aide d'un réseau (GILLET, 2008: 159).

1.2.2. Les postes ordinateurs ou micro ordinateurs

Ce sont les ordinateurs de bureau et leurs périphériques 'imprimantes, souris, fax, téléphones, etc.) d'entrée/sortie, les ordinateurs portables, les ordinateurs de poche, les

tablettes et les Smartphones qui permettent de se connecter de n'importe quel lieu où une connexion réseau est disponible (DAYAN & Al, 2004).

1.2.3. Les équipements électroniques

Selon CARPENTIER (2009), les équipements électroniques sont un ensemble constitué de tous les appareils électroniques qui peuvent être intégrés au système informatique. Il s'agit principalement des imprimantes, des scanners, des vidéo projecteurs, des appareils fax, des téléphones, des photocopieurs, des caméras numériques, des clés USB, des lecteurs, des disques externes, etc.

1.2.4. L'infrastructure réseau

Un réseau informatique peut être défini comme un ensemble d'équipements reliés entre eux pour échanger des informations. Selon YADAV & SINGH (2009), les infrastructures réseaux ou supports peuvent être sur des câbles dans lesquels circulent des signaux électriques, l'atmosphère (ou le vide spatial) où circulent des ondes radio, ou des fibres optiques qui propagent des ondes lumineuses, des modems et des antennes réseaux. Elles permettent de relier «physiquement» des équipements assurant l'interconnexion des moyens physiques qui sont définis par des protocoles.

Les protocoles de communication définissent de façon formelle et interopérable la manière dont les informations sont échangées entre les équipements du réseau. Des logiciels dédiés à la gestion de ces protocoles sont installés sur les équipements d'interconnexion qui sont par exemple les commutateurs réseau (Switch), des concentreurs (Hub), les routeurs, les commutateurs téléphoniques, etc.

1.2.5. La salle informatique

Selon YADAV & SINGH (2009), c'est une salle, en général, aménagée pour la circonstance et qui héberge tous les équipements informatiques, spécialisés ou non, nécessaires au déploiement des ressources informatiques. On trouve dans cette salle les serveurs, calculateurs, solutions de sauvegarde et de restauration des données, baies de stockage, pour ne citer que ceux-là. Cette salle contient également les éléments fondamentaux

du réseau à savoir les commutateurs, routeurs et autres ainsi que les points d'accès et équipements servant à connecter la société avec le monde extérieur (central téléphonique, accès internet, etc.).

1.2.6. Les applications informatiques

Selon GILLET (2008), une application opérationnelle gère un processus. Celui-ci se déroule, le plus souvent, de manière transversale par rapport aux services.
Le groupe de travail lié au processus est constitué d'acteurs appartenant à différents services.
Une application informatique correspond donc à une organisation qui comprend, en règle générale, des programmes, des fichiers, des instructions d'exécution, des paramètres, des tables, une documentation,... et qui permet d'exécuter des traitements dans toutes les fonctions de l'entreprise.

1.3. La fonction informatique: rôle et organisation

Du fait de son caractère stratégique, la fonction informatique doit jouer un rôle central dans le pilotage et la gestion des systèmes d'information. Elle doit, notamment, assurer l'alignement de la stratégie informatique avec celle de l'entreprise.

1.3.1. Rôle de la fonction informatique dans l'entreprise

Selon GILLET (2008), la fonction informatique est responsable de la disponibilité des moyens techniques adéquats et a pour objectif de rendre des services aux utilisateurs. En tout état de cause, le rôle de la fonction informatique diffère selon la taille et le degré de maturité de l'organisation informatique. En fait, quelque soit la structure adoptée par l'organisation, la fonction informatique doit assurer au moins deux principales activités à savoir:

- la gestion des moyens et opérations d'exploitation informatiques;
- la gestion des opérations relatives à l'acquisition, le développement et la maintenance des systèmes d'information;

Plus généralement, la fonction informatique est organisée de la façon suivante:

- une direction ou service en charge de la supervision de l'unité ou entité informatique;
- une division ou service ou section exploitation en charge des travaux d'exploitation;

- une division ou service ou section études et développement en charge de la gestion des projets informatiques;
- une division ou service ou section systèmes en charge de la gestion et de la maintenance des systèmes informatiques.

1.3.2. Les principales attributions de la fonction informatique

Les objectifs assignés à la fonction informatique peuvent être résumés comme suit:

- permettre à l'informatique de délivrer un bon niveau de service aux utilisateurs et de pouvoir répondre à leurs attentes, en termes de qualité et délais, en formalisant les relations et les responsabilités dans le domaine informatique des différents intervenants (personnel, ressources informatiques, organisation, utilisateurs);
- assurer un bon niveau de contrôle des opérations de la direction informatique, en formalisant les contrôles du personnel informatique et les tableaux de bord de la direction informatique;
- assurer la pérennité des opérations de la direction informatique en formalisant les procédures informatiques et les systèmes de sécurité;
- assurer un bon niveau de fonctionnement des applications informatiques.

A cet effet, la structure en charge de la fonction informatique définit et met en œuvre les systèmes d'information destinés au pilotage et à la gestion des différentes activités de l'organisation. A ce titre, elle est chargée de définir, de mettre en place et de gérer les moyens techniques nécessaires aux systèmes d'information et de communication, et de panifier leur évolution dans le cadre d'un schéma directeur (GILLET, 2008).

Elle définit et met en œuvre également les contrôles et les ressources informatiques (personnel, application; technologie, utilitaires, données) qui permettent d'atteindre ses objectifs dans les domaines ou processus suivants (DESMOULINS, 2009):

- le planning et l'organisation;
- l'acquisition et la mise en service;
- l'exploitation et la maintenance;
- le pilotage des activités informatiques.

Les contrôles mis en place doivent être suffisants pour permettre de prévenir, détecter et corriger les risques auxquels sont exposées les ressources informatiques de l'organisation.

1.4. Les risques informatiques

Les risques informatiques font partie des risques opérationnels. Ils peuvent être assimilés à «tout évènement qui, affectant un système informatique, est susceptible d'entrainer des dommages et/ou des pertes à l'entreprise concernée» (IFACI, 1990: 24).
Ces risques trouvent leurs origines dans les causes suivantes:

- les causes accidentelles, naturelles ou techniques;
- les erreurs humaines;
- les malveillances, internes ou externes, involontaires ou volontaires.

Aussi, les évènements tels que les grèves des employés ou le départ ou disparition de personnel stratégique dans la chaîne du processus informatique est aussi une des causes majeures des risques informatiques (CLUSIB, 2006: 13).

1.4.1. Les risques d'origine accidentelle

Ces risques sont d'ordre matériel ou sont relatifs aux pannes et dysfonctionnements de matériel ou de logiciel de base. Selon CLUSIB (2006), ce sont des risques matériels se traduisent par la destruction totale ou partielle d'un ou de plusieurs composants d'un système d'information, pouvant provoquer, l'indisponibilité plus ou moins prolongée du système. Il peut s'agir aussi des défaillances, pannes et dysfonctionnements de matériel ou logiciel de base pouvant provoquer des interruptions de service.

1.4.2. Erreurs humaines

Pour CLUSIB (2006), les risques informatiques ayant pour origines les erreurs humaines peuvent être de différentes natures à savoir, principalement:

- erreurs de saisie, de transmission et d'utilisation de l'information;
- erreurs d'exploitation;
- erreurs de conception et de réalisation.

Ces erreurs prennent des formes variées telles que effacement accidentel des fichiers, supports ou copies de sauvegarde, chargement d'une version incorrecte de logiciel ou de copie de sauvegarde, lancement d'un programme inapproprié, etc. Il est en général difficile d'identifier la cause exacte de ces problèmes, cause qui peut être une faute professionnelle, malveillance, erreur, négligence, laxisme, ou autres.

Les erreurs de conception dans la configuration et le paramétrage des systèmes de protection engendrent de grosses vulnérabilités. Il en va par exemple d'ordinateurs coupe- feu "*firewalls*" ne filtrant rien ou peu ou encore qui soient mal placés dans le réseau.
Un "*firewall*" (pare-feu ou coupe-feu) est un système qui permet de bloquer et de filtrer les flux qui lui parviennent, de les analyser et de les autoriser s'ils remplissent certaines conditions, de les rejeter dans le cas contraire.

Des faiblesses dans la conception de la protection logique, telles que des mots de passe communs à plusieurs personnes ou trop faciles à découvrir (par «craquage» ou piratage, par observation illicite,...) créent également des brèches dans la sécurité.
Le recours à des systèmes automatisés de gestion des applications permet de réduire le rôle joué par les opérateurs humains et de faire baisser le nombre de ces erreurs.

1.4.3. Malveillance

Selon GHERNAOUTI-HELIE (2006), la malveillance est définie comme des «actions à caractère hostile pouvant porter atteinte aux ressources d'une organisation qui peuvent être commises directement ou indirectement par des personnes internes ou externes à celle-ci». Il s'agit, entre autres, de vol et sabotage de matériels, de données, divulgation d'informations confidentielles, fraudes, intrusions illicites, indiscrétions et détournements d'information et de logiciels, etc.

1.4.4. Grève, départ de personnel stratégique, pénurie de personnel.

Selon CLUSIB (2006), le personnel est un maillon indispensable dans la chaîne qui assure le fonctionnement d'un système d'information. L'indisponibilité ou la disparition d'un membre de personnel-clé peut provoquer l'arrêt du système et par voie de conséquence celle de toute l'activité de l'entreprise.

1.5. Les conséquences des risques informatiques.

Il s'agit des pertes, directes et/ou indirectes, subies par l'entreprise suite à des sinistres d'origine accidentelle, des erreurs ou malveillances (IFACI, 1990). Dans tous les cas, les conséquences d'atteinte aux systèmes d'information sont multiples.

1.5.1. Les pertes directes.

De façon directe, elles correspondent à une disparition d'actifs (IFACI, 1990). Elles peuvent être des pertes directes matérielles (équipements informatiques ou télématiques; bâtiments; logiciels; données....) ou des pertes directes immatérielles (contenus de logiciels et/ou données).

1.5.2. Les pertes indirectes.

Selon CLUSIB (2006), les conséquences indirectes matérielles d'un incident sont aussi importantes si non plus que les pertes directes. Il s'agit des charges telles que les frais de constitution des données; les frais supplémentaires de traitement informatique après sinistre; les pertes d'exploitation; les frais d'études et d'expertise; etc.

Quant aux pertes indirectes immatérielles, elles concernent essentiellement l'atteinte à l'image de marque et donc le risque de fuite de la clientèle, le retard technologique, la perte de marchés potentiels.

1.6. Les dispositifs de maîtrise des risques et de contrôle interne informatiques

Les dispositifs de maîtrise des risques et de contrôle interne participent de manière complémentaire à la maîtrise des activités de l'organisation. Selon IFACI, COOPERS & LYBRAND (1994), le dispositif de maîtrise des risques vise à identifier et analyser les principaux risques de la société. Il intègre des plans d'action qui peuvent prévoir la mise en place de contrôles, un transfert des conséquences financières (mécanisme d'assurance par exemple) ou une adaptation de l'organisation. Les contrôles à mettre en place relèvent du dispositif de contrôle interne. De son côté, le dispositif de contrôle interne s'appuie sur le dispositif de gestion des risques pour identifier les principaux risques à maîtriser.

1.6.1. Le Dispositif de maîtrise des risques

Selon le cadre de référence AMF (2010), le dispositif de maîtrise des risques existant dans une société, doit comprendre un ensemble de moyens, de comportements, de procédures et d'actions adaptés aux caractéristiques de l'organisation.
En effet, il permet aux dirigeants de maîtriser les risques encourus ou, du moins, de les maintenir à un niveau acceptable.

Selon IFACI, PRICEWATERHOUSECOOPERS & AL (2005: 5), «le contrôle interne est conçu pour identifier les évènements potentiels susceptibles d'affecter l'organisation et pour gérer les risques dans la limité de son appétence pour le risques».
Ce dispositif doit prévoir, entre autres, les aspects suivants:

- un cadre organisationnel comprenant:
  - une organisation qui définit les rôles et responsabilités des acteurs, établit les procédures et les normes claires et cohérentes du dispositif;
  - une politique de gestion des risques qui formalise les objectifs du dispositif, la démarche d'identification, d'analyse et de traitement des risques, les limites que la société détermine;
  - un système d'information qui permet la diffusion en interne d'informations relatives aux risques.
- un processus de maîtrise des risques comprenant les étapes suivantes:
  - identification des risques, étape permettant de recenser et de centraliser les principaux risques menaçant l'atteinte des objectifs;
  - analyse des risques, étape consistant à examiner les conséquences potentielles des principaux risques;
  - traitement du risque, étape permettant de choisir le(s) plan(s) d'action le(s) plus adapté(s) à la société;
- Un pilotage en continu du dispositif de maîtrise des risques en ce sens que le dispositif de gestion des risques fait l'objet d'une surveillance et d'une revue régulière, son suivi permet l'amélioration continue du dispositif.

1.6.2. Le contrôle interne informatique

Le contrôle interne informatique fait partie intégrante du dispositif de maîtrise des risques ou peut être considéré comme son complément indispensable. Selon IFACI, COOPERS & LYBRAND (1994), c'est un processus mis en œuvre par le conseil d'administration, les dirigeants et le personnel d'une organisation, destiné à fournir une assurance raisonnable quant à l'atteinte des objectifs suivants:

- la réalisation et l'optimisation des opérations;
- la fiabilité des informations financières;
- la conformité aux lois et règlements en vigueur.

D'une façon générale, le contrôle interne contribue à la maîtrise des activités de l'organisation, à l'efficacité de ses opérations et à l'utilisation efficiente de ses ressources. Il appartient donc à chaque organisation de mettre en place un dispositif de contrôle interne adapté à sa situation (AMF, 2010).

Ce dispositif doit prévoir, entre autres:

- *une organisation* comportant une définition claire des responsabilités, disposant des ressources et des compétences adéquates et s'appuyant sur des procédures, des systèmes d'information, des outils et des pratiques appropriés;
- *la diffusion en interne d'informations pertinentes*, fiables, dont la connaissance permet à chacun d'exercer ses responsabilités;
- *un système visant à recenser et analyser les principaux risques* identifiables au regard des objectifs de la société et à s'assurer de l'existence de procédures de gestion de ces risques;
- *des activités de contrôle proportionnées* aux enjeux propres à chaque processus et conçues pour réduire les risques susceptibles d'affecter la réalisation des objectifs de l'organisation;
- *une surveillance permanente* du dispositif de contrôle interne ainsi qu'un examen régulier de son fonctionnement. Cette surveillance qui peut utilement s'appuyer sur la fonction d'audit interne de la société lorsqu'elle existe, peut conduire à l'adaptation du dispositif de contrôle interne (SCHICK, 2010: 22).

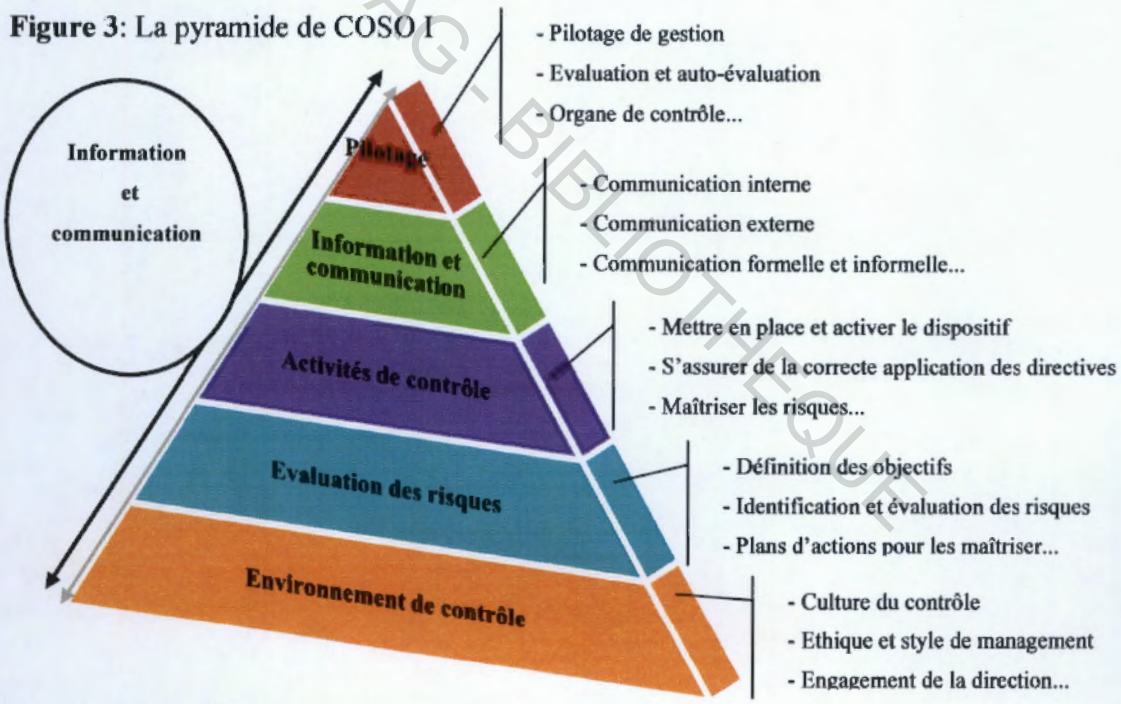
1.6.3. Les composantes du contrôle interne

Selon IFACI, COOPERS & LYBRAND (1994), le contrôle interne est constitué de cinq composantes à savoir:

- l'environnement de contrôle;
- l'évaluation des risques;
- les activités de contrôle;
- l'information et la communication;
- le pilotage ou la surveillance, c'est-à-dire le «contrôle du contrôle» interne.

Chacune de ces composantes se décline ensuite en un certain nombre d'éléments concourant à la réalisation des objectifs de l'organisation, comme le traduit la figure 3 ci-dessous.

Figure 3: La pyramide de COSO I



Source : Nous-mêmes, adapté de SCHICK (2010. 19)

1.6.3.1. L'environnement de contrôle interne

Selon IFACI, COOPERS & LYBRAND (1994), l'environnement de contrôle est un élément très important de culture d'une organisation, puisqu'il reflète son style et détermine le niveau de sensibilisation du personnel au besoin de contrôles. Il constitue, de ce fait, le

fondement structurel de tous les autres éléments du dispositif de management des risques, imposant discipline et organisation.

Selon, AFAI (2008: 50), «Le contrôle informatique s'appuie sur l'environnement de contrôle de l'organisation et concerne l'attribution de l'autorité et de la responsabilité des activités. Les solutions de gestion des identités et des accès sont un élément essentiel du dispositif.». C'est dire que l'environnement de contrôle exerce une influence profonde sur la façon dont les activités sont structurées, la définition des objectifs et l'évaluation des risques.

1.6.3.2. Evaluation des risques

Toute organisation s'expose à une multitude de risques tant externes qu'internes. L'analyse des risques est le processus qui identifie et évalue ces risques par rapport aux objectifs de l'organisation et constitue dès lors une base pour le contrôle interne informatique.

L'évaluation des risques informatiques intervient (AFAI, 2008):

- au niveau de l'organisation avec des processus d'évaluation des risques des systèmes d'information couvrant le management, la sécurité des données, et le développement informatiques;
- au niveau de chaque activité: l'exploitation des infrastructures informatiques, les processus de modification d'une application.

1.6.3.3. Activités de contrôle

Les normes et procédures de contrôle doivent être élaborées et appliquées pour s'assurer que sont exécutées efficacement les mesures identifiées par le management comme nécessaires à la réduction des risques liés à la réalisation des objectifs.

Le COSO II REPORT identifie deux grands groupes d'activités de contrôle interne informatique que sont les contrôles généraux et les contrôles applicatifs.
Les contrôles généraux se rapportent au contrôle interne appliqué à la fonction informatique. Ils concernent les points suivants:

- la planification et l'organisation générale de l'activité informatique;
- la conception et le développement des applications

- la maintenance des matériels, des applications et des systèmes;
- les accès aux ressources matérielles et informationnelles (données et programmes);
- les autres contrôles de données et les procédures affectant les opérations informatiques globales.

Les contrôles applicatifs, quant à eux, sont conçus pour contrôler le bon fonctionnement des applications informatiques. Ils permettent de s'assurer l'exhaustivité et l'exactitude des traitements des transactions, leur autorisation et leur validité (AFAI, 2008).

1.6.3.4. Information et communication

Selon IFACI, COOPERS & LYBRAND (1994), cette composante vise à assurer que l'information pertinente est identifiée, recueillie et diffusée dans les délais appropriés afin que l'ensemble du personnel puisse assumer ses responsabilités. Pour cela, les systèmes d'information doivent garantir que toutes les informations importantes sont collectées de manière fiable et diffusées convenablement.

1.6.3.5. Pilotage du contrôle interne

Les systèmes de contrôle interne doivent être supervisés pour évaluer leur qualité et leur performance dans le temps. Pour cela, il convient de mettre en place un système de pilotage permanent, de procéder à des évaluations périodiques ou encore de combiner les deux. Le pilotage permanent s'inscrit dans le cadre des activités courantes et comprend des contrôles réguliers effectués par le management et le personnel d'encadrement, ainsi que d'autres techniques utilisées par le personnel à l'occasion de ses travaux (IFACI, COOPERS & LYBRAND, 1994).

1.6.4. Les acteurs du contrôle interne informatique

Le contrôle interne est l'affaire de tous, des organes de gouvernance à l'ensemble des collaborateurs de la société. C'est dire que tous les membres du personnel ont une responsabilité, plus ou moins importante, en matière du contrôle interne. Toutefois et en tout état de cause, la responsabilité du système de contrôle interne incombe au management et, au premier rang, au Président Directeur Général (IFACI, COOPERS & LYBRAND, 1994).

1.6.4.1. Le Conseil d'Administration

En matière de contrôle interne, le niveau d'implication des conseils d'Administration varie d'une organisation à l'autre. En tout état de cause, il revient à la Direction Générale ou au Directoire de rendre compte au conseil des caractéristiques essentielles du dispositif de contrôle interne.

1.6..4.2. La Direction Générale

La Direction générale est chargée, en principe, de définir, d'impulser et de surveiller le dispositif le mieux adapté à la situation et à l'activité de l'organisation. La Direction Générale, dans ce cadre, se tient régulièrement informée des dysfonctionnements de la société, de ses insuffisances et des difficultés d'application, voire de ses excès, et veille à l'engagement des actions correctives nécessaires.

1.6.4.3. L'audit interne

Lorsqu'il existe, le service d'audit interne a la responsabilité d'évaluer l'efficacité des fonctionnements des dispositifs de maîtrise des risques et de contrôle interne et de formuler toutes recommandations pour les améliorer, dans le champ couvert par ses missions. Il n'est pas directement impliqué dans la mise en place et la mise en œuvre quotidienne de ces dispositifs (AMF, 2010).

1.6.4.4. Le personnel de l'entreprise

Chaque collaborateur concerné devrait avoir la connaissance et l'information nécessaires pour établir, faire fonctionner et surveiller le dispositif de contrôle interne, au regard des objectifs qui lui ont été assignés.

1.6.4.5. Limites du contrôle interne

Selon AMF (2010), le dispositif de contrôle interne aussi bien conçu et aussi bien appliqué soit-il, ne peut fournir une garantie absolue quant à la réalisation des objectifs de la société. La probabilité d'atteindre ces objectifs ne relève pas de la seule volonté de la société.

Selon IFACI, PRICEWATERHOUSECOOPERS & AL (2005), Il existe, en effet, des limites inhérentes à tout système de contrôle interne. Ces limites résultent de nombreux facteurs, notamment des incertitudes du monde extérieur, de l'exercice de la faculté de jugement ou de dysfonctionnements pouvant survenir en raison d'une défaillance humaine ou d'une simple erreur. Des actes de collusion sont toujours possibles, par exemple, une entente entre plusieurs personnes peut se traduire par des défaillances dans le dispositif de management des risques. En outre, lors de la mise en place des contrôles, il est nécessaire de tenir compte du rapport coût/bénéfice afin de ne pas développer des systèmes de contrôle interne inutilement coûteux.

Conclusion

Les risques informatiques, comme tous les risques opérationnels, constituent des menaces réelles ou potentielles, redoutables et permanentes, pesant sur le dispositif informatique de l'entreprise, véritable support transversale de ses processus.

La survenance de ces risques peut conduire à une perturbation du déroulement normal des processus métiers et générer des pertes financières et/ou matérielles considérables ou une dégradation de l'image de l'entreprise. Il convient dès lors, d'identifier ces risques au travers des processus informatiques de l'entreprise, de les évaluer afin de décider des mesures adéquates à prendre pour les réduire et se couvrir contre les risques résiduels.

CHAPITRE II: DEMARCHE THEORIQUE D'EVALUATION DES RISQUES INFORMATIQUES

Introduction

Le système d'information de l'entreprise s'appuie, pour l'essentiel, sur le dispositif informatique, considéré comme son principal support. Or celui-ci est exposé à des nombreux risques qui menacent son bon fonctionnement, que ces derniers soient inhérents (environnement) ou liés aux dispositifs de contrôle (applications) conçus et mis en œuvre. Dès lors, il convient d'identifier ces risques, de les analyser et de les évaluer afin de prendre des mesures en vue de leur réduction, suppression ou acceptation, s'il y a lieu. Dans cette perspective, le présent chapitre sera consacré à la démarche d'évaluation des risques.

L'objectif recherché, dans cette démarche, est d'élaborer une cartographie des risques destinée à être utilisée comme outil de communication et de gestion des risques de l'entité ou de l'organisation concernée.

2.1. Cartographie des risques informatiques

La cartographie des risques peut être définie comme un document permettant de recenser les principaux risques d'une organisation et de les présenter synthétiquement sous une forme hiérarchisée pour assurer une démarche globale d'évaluation des risques.

Selon JIMENEZ (2008), les objectifs visés par la cartographie des risques sont:

- d'évaluer les risques identifiés en termes de gravité et de probabilité;
- de calculer le score de chaque risque;
- de classer, de comparer et de hiérarchiser les risques entre eux;
- de définir un plan d'action de gestion des risques en fonction des ressources disponibles et d'en assurer le suivi (IFACI, PRICEWATERHOUSE & AL, 2005);
- de communiquer les informations sur les risques de l'organisation aux dirigeants.

Pour DESROCHES & AL. (2003:56). «Les études de risques ont pour but de:

- identifier les risques, à priori, susceptibles de se produire lors du fonctionnement d'un système ou du déroulement d'une activité;
- évaluer leur probabilité et la gravité de leurs conséquences;
- aider à définir et à consolider les actions pouvant les maîtriser;
- aider à définir les actions permettant de garder dans le temps le risque à un niveau acceptable.»

C'est dire que dans l'optique de maîtrise des risques, l'élaboration d'une cartographie constitue une étape importante dans le processus de gestion des risques d'une organisation.

2.2. Démarche d'élaboration d'une cartographie des risques

Selon JIMENEZ (2008: 63), «la cartographie des risques consiste à associer aux processus les évènements à risques qui peuvent entraîner une perte... en donnant une vision des impacts possibles et le degré de maîtrise estimé.». Les étapes de la démarche d'élaboration de la cartographie préconisée par cet auteur sont les suivantes:

- définir le couple processus/risque à évaluer;
- identifier et évaluer les risques bruts;
- apprécier le dispositif de maîtrise des risques;
- assurer un contrôle de cohérence avec les risques bruts;
- classifier et hiérarchiser les risques selon les différents angles d'analyse possibles.

Selon SCHICK (2010: 64), «la réalisation d'une cartographie des risques dans une organisation permet d'avoir une vision d'ensemble, exhaustive et précise, de son exposition aux turbulences de toutes natures, tant internes qu'externes. ..., cette approche permet par ailleurs de définir les dispositifs adéquats à mettre en place pour maîtriser ces risques.».

Nous reprenons ici les six étapes classiques suivies dans l'élaboration d'une cartographie des risques proposées par SCHICK (2010), à savoir:

Etape 1: identification et description des « ensembles homogènes » (métiers, entités, processus) caractéristiques de l'organisation, fonction ou entité concernée.

Cette première étape aboutit à l'élaboration d'une cartographie des « ensembles homogènes » ou un découpage homogène des processus métier.

Etape 2: identification et évaluation des risques inhérents ou bruts.

Un risque, inhérent ou brut, est ainsi qualifié lorsqu'il est apprécié dans l'absolu indépendamment des dispositions existantes pour en réduire l'impact et/ou la probabilité.

Il s'agit, au cours de cette étape, de réaliser les travaux suivants:

- élaborer une typologie des risques;
- définir une échelle de cotation des risques pour les deux paramètres caractéristiques à savoir l'impact (en termes de gravité) et l'occurrence (en termes de probabilité).

Par exemple une échelle de 1 à 4 en fonction des critères suivants (SCHICK, 2010):

- **Echelle «impact»:**

1 = faible: pas de conséquence sur les valeurs, les objectifs stratégiques ou les actifs de l'organisation.

2 = Modéré: risque présentant un impact surmontable.

3 = Significatif: risque pouvant avoir un impact significatif sur les valeurs, les objectifs stratégiques ou les actifs de l'organisation.

4 = Extrême: risque ayant un impact grave sur les valeurs, les objectifs stratégiques et les actifs de l'organisation.

- **Echelle «occurrence»:**

1 = Faible: risque jamais apparu ou ayant une faible probabilité d'apparition.

2 = Peu probable: risque jamais apparu mais qui peut se manifester.

3 = Probable: risque apparu ou qui pourrait se manifester compte tenu du contexte.

4 = Très élevé: très forte probabilité ou fréquence d'apparition.

Pour chaque « ensemble homogène » et pour chaque nature de risque, il y a lieu de:

- procéder à une cotation de l'impact et de l'occurrence;
- formaliser les résultats dans une matrice des risques bruts (risques inhérents).

Etape 3: identification et évaluation des dispositifs de contrôle interne présents dans l'organisation.

Pour chaque «ensemble homogène» et au regard du chaque risque:

- identifier les dispositifs de contrôle interne existants;
- définir une échelle de cotation pour l'évaluation du contrôle interne par rapport à sa capacité de maîtrise des risques.

Par exemple une échelle de 1 à 4 en fonction des critères suivants (SCHICK, 2010):

1 = Non maîtrise: absence de pilotage de l'organisation et de formulation des procédures, compétences insuffisantes

2 = Maîtrise partielle: pilotage empirique, esquisse de formulation des procédures, compétences partielles.

3 = Maîtrise correcte: pilotage existant mais perfectible, procédures existantes mais perfectibles, compétences dans le domaine.

4 = Très bonne maîtrise: pilotage institutionnelle performante, procédures rédigées, diffusées, appliquées et mises à jour régulièrement.

Il y a lieu, au cours de cette étape de:

- procéder à une cotation des dispositifs de contrôle interne existants;
- formaliser les résultats dans une matrice d'évaluation du contrôle interne.

Etape 4: évaluation des risques résiduels, c'est-à-dire ceux qui subsistent après prise en compte de la dimension contrôle interne existante.

Un risque résiduel correspond à un risque brut non couvert ou mal couvert par un dispositif de contrôle interne absent ou défaillant (SCHICK, 2010: 67).

En définitive, on obtient en formalisant, une cartographie des risques pour l'entité concernée. La cartographie ainsi obtenue peut constituer un excellent outil de reporting, de gestion des risques et des ressources.

Etape 5: décision d'acceptation du risque ou définition et mise en œuvre de nouveaux dispositifs de prévention, de réduction ou de protection pour en assurer la maîtrise.

Selon IFACI, PRICEWATERHOUSECOOPERS & AL. (2005), Il s'agit, une fois les risques identifiés et évalués, de déterminer «quels traitements appliquer à chacun de ces risques». Les différentes solutions possibles sont:

- *l'évitement*: cesser les activités à l'origine du risque;
- *la réduction*: prendre des mesures afin de réduire la probabilité d'occurrence et/ou l'impact. Il s'agit habituellement d'une multitude de décisions prises quotidiennement;
- *le partage*: diminuer la probabilité ou l'impact d'un risque en transférant ou en partageant le risque. Parmi les techniques courantes, il y a l'achat de produits d'assurances, les opérations de couverture ou l'externalisation d'une activité;

- *l'acceptation*: ne prendre aucune mesure pour modifier la probabilité d'occurrence du risque et son impact (IFACI, PRICEWATERHOUSECOOPERS & AL, 2005: 84).

Etape 6: mise en place d'un système de reporting des résultats obtenus à la hiérarchie concernée (SCHICK, 2010).

D'une façon générale, la mise en place d'un système de reporting comprend principalement les volets suivants:

- reporting initial au management sur les risques résiduels;
- reporting consolidé (pour la formalisation de la cartographie globale);
- reporting sur la mise en œuvre des plans d'action.

2.2.1. Identification et découpage de processus informatiques

Cette partie fera l'objet de notre étude pendant la phase pratique, en particulier lors de la prise de connaissance générale de la fonction informatique. A l'issue de cette étape de prise de connaissance, les principaux processus gérés par la fonction informatique seront identifiés et décrits en détail. Mais d'ores et déjà, compte tenu des attributions de la fonction informatique dans une organisation de certaine taille, les domaines ou processus suivants peuvent être retenus (DESMOULINS, 2009):

- organisation et pilotage de la fonction informatique;
- sécurité et gestion des incidents informatiques;
- exploitation informatique:
- maintenance informatique;
- développement et mise en services des applications informatiques.

2.2.2. Identification et évaluation des risques inhérents

Selon IFACI, PRICEWATERHOUSECOOPERS & AL. (2005: 204), «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».

Il s'agit de tout évènement potentiel, d'origine interne ou externe pouvant être un incident, une occurrence qui affecte l'atteinte des objectifs ou la mise en œuvre de la stratégie de l'organisation. Plusieurs approches et techniques, utilisées individuellement ou en combinaison permettent d'identifier ces évènements à risque.

2.2.2.1. Techniques d'identification des risques

Selon IFACI, PRICEWATERHOUSECOOPERS & AL. (2005), «La méthodologie d'identification des évènements d'une organisation peut comprendre une combinaison des techniques et d'outils.
Par exemple le management peut mettre en place des groupes de travail interactifs, comme outil de sa méthodologie d'identification des évènements....».

L'identification des processus et des risques associés nécessite de prendre en compte deux méthodes, à savoir l'approche «Bottom-up» et l'approche «Top-down».
Pour l'approche «bottom-up ou méthode ascendante», l'identification est effectuée par les opérationnels proches de l'activité et remonte vers les personnes en charge de l'élaboration de la cartographie des risques. Quant à l'approche «Top-down», les personnes en charge de l'élaboration de la cartographie des risques vont descendre sur le terrain chercher l'information auprès des opérationnels.

En tout cas, plusieurs techniques permettent l'identification et l'évaluation des risques inhérents. Il convient de retenir, entre autres:

- identification basée sur les actifs créateurs de valeurs (risques associés aux actifs intangibles).
- identification basée sur l'atteinte des objectifs (un risque peut empêcher l'atteinte des objectifs; ces derniers sont d'abord définis, avant de leur associer les menaces pesant sur eux).
- identification basée sur les check-lists: liste déjà préconçue qui énumère l'ensemble des risques possibles afin de voir si chaque risque concerne l'entité ou pas.
- identification par analyse historique: identification en se basant sur les risques opérationnels déjà survenus au sein de l'entité.
- identification basée sur l'analyse de l'environnement (menaces de l'environnement économique, technologique…).
- identification par analyse des activités: décomposition des processus en activités identification des risques associés (conséquences potentielles de la non/mauvaise exécution des tâches).
- Identification par groupe de travail et entretiens: techniques permettant d'identifier les évènements en exploitant les connaissances et l'expérience des collaborateurs.

2.2.2.2. Evaluation des risques inhérents

L'évaluation des risques consistent à déterminer dans quelles mesures les évènements potentiels sont susceptibles d'avoir un impact sur la réalisation des objectifs et d'évaluer la probabilité d'occurrence et d'impact de ces évènements (PRICEWATERHOUSECOOPERS, IFACI & AL, 2005: 73).

L'évaluation des risques peut être effectuée en utilisant les techniques qualitatives ou quantitatives. Les techniques d'évaluation qualitatives sont souvent utilisées lorsque les risques ne se prêtent pas à une quantification ou lorsqu'il n'y a pas suffisamment de données fiables pour effectuer une évaluation quantitative.

Exemples de techniques quantitatives couramment utilisées :

- *benchmarking*: Il s'agit d'un processus d'échange d'information au sein d'un groupe d'entités qui repose sur des critères communs. Il porte sur des évènements, des processus spécifiques ou sur la comparaison de mesures et de résultats et permet d'identifier des opportunités d'amélioration. Les données collectées sur les évènements, les processus et les indicateurs de mesure sont utilisés pour évaluer la probabilité de survenance et l'impact de certains évènements dans leur secteur d'activité.
- *modèles probabilistes* : Les modèles probabilistes associent une probabilité d'occurrence à un certain nombre d'évènements et à leurs impacts, sur la base de certaines hypothèses. La probabilité d'occurrence et l'impact résultant d'un évènement sont évalués sur la base des données historiques...
- *modèles non-probabilistes* : Les modèles non probabilistes utilisent des hypothèses subjectives afin d'estimer l'impact d'évènement sans quantifier l'occurrence.

Le risque et ses conséquences sont mesurables selon deux dimensions, à savoir:

- l'occurrence ou la probabilité de survenance du risque;
- l'impact ou la conséquence du risque s'il se matérialise, il s'agit de quantifier la conséquence de celui-ci.

A cet effet, selon SCHICK (2010), l'échelle de cotation de 1 à 4 peut être retenue pour l'évaluation en fonction des critères définis sur les deux tableaux (probabilité/occurrence et impact) de la page suivante:

Tableau 1: Echelle «probabilité/occurrence» des risques

Cote	Probabilité / Fréquence	Critère d'évaluation survenance
1	Faible (très peu probable)	Risque jamais apparu ou ayant une faible probabilité d'apparition.
2	Peu probable	Risque jamais apparu mais qui peut se manifester
3	Probable (possible)	Risque apparu ou qui pourrait se manifester compte tenu du contexte.
4	Très probable (quasi certain)	Très forte probabilité ou fréquence d'apparition.

Source: Nous-mêmes, adapté de SCHIK (2010: 67).

Tableau 2: Echelle «impact» des risques

Cote	Impact/Gravité	Critère d'évaluation conséquence
1	Faible (mineur)	Pas de conséquence sur les valeurs, les objectifs stratégiques ou les actifs de l'organisation.
2	Modéré	Risque présentant un impact surmontable
3	Significatif (majeur)	Risque pouvant avoir un impact significatif sur les valeurs, les objectifs stratégiques ou les actifs de l'organisation.
4	Extrême (critique)	Risque ayant un impact très grave sur les valeurs, les objectifs stratégiques et les actifs de l'organisation.

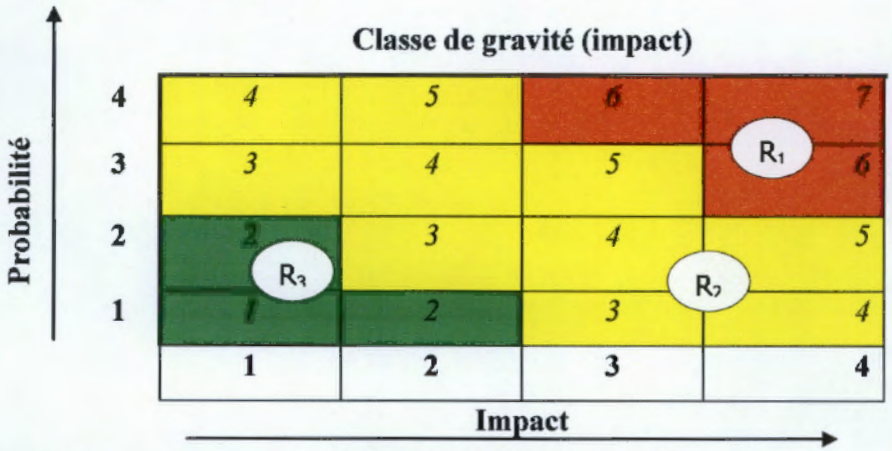
Source: Nous-mêmes, à partir de SCHICK (2010: 67).

2.2.2.3. Hiérarchisation des risques inhérents

Pour hiérarchiser les risques inhérents ou résiduels (si l'évaluation est faite à la fois), il y a lieu de calculer le score ou le coefficient de ces risques. Ce qui permet d'évaluer leurs criticités. Selon DESROCHES (2003), à partir des classes de probabilité/occurrence placées en ordonnées et des quatre classes de gravité (impact) placées en abscisses, on définit les criticités des scénarios.... En d'autres termes, il s'agit de:

- cotation des risques (calcul de score des risques par le produit de leurs dimensions ou calcul de leurs coefficients);
- classement des risques par ordre de score décroissant.

Tableau 3: Tableau de classification risques inhérents



Sources: Nous-mêmes, à partir de DESROCHES (2003).

Les risques sont regroupés en trois classes selon leurs criticités comme visualisées sur le tableau des risques ci-dessus. Le classement ou la hiérarchisation des risques par ordre de priorité est la suivante:

R_1= 6 à 7: Risque Elevé

R_2 = 3 à 5: Risque Modéré

R_3= 1 à 2: Risque Faible

Ce classement permet d'obtenir une matrice des risques inhérents.

Tableau 4: Matrice d'évaluation des risques inhérents

Classe de criticité		Cote	Type de risque	Niveau de risque	Action
R_3	1 à 2	1	Faible	Acceptable en l'état	Aucune action nécessaire
R_2	3 à 5	2	Modéré	Acceptable sous contrôle	A maîtriser
R_1	6 à 7	3	Elevé	Inacceptable	Rejeter les évènements et empêcher les scénarios y conduisant (à maîtriser)

Source: Nous-mêmes; adapté de DESROCHES (2003).

La décision de l'acceptabilité du risque initial (inhérent) ou résiduel est faite sur la base des estimations des criticités (DESROCHES, 2003:50).

2.2.3. Identification et évaluation des dispositifs de contrôle interne existants

Au regard des risques évalués et hiérarchisés, il importe de procéder à l'évaluation des dispositifs de contrôle interne existants par rapport à leur capacité de maîtrise des risques. Cette démarche consiste à réaliser les travaux suivants:

- identification des contrôles internes présents dans l'organisation (SCHICK, 2010), mis en œuvre pour pallier les conséquences négatifs des risques;
- identification des objectifs de ces contrôles et des risques inhérents couverts;
- évaluation de la qualité de ces contrôles (JIMENEZ, 2008).

2.2.3.1. Identification des contrôles existants et de leurs objectifs

Les dispositifs de contrôles internes existants dans une organisation doivent comprendre plusieurs types de contrôles, chacun, visant des objectifs bien déterminés, à savoir:

- contrôles de prévention: ils visent à réduire la probabilité de survenance de ce risque. Ils agissent sur la cause de ce risque pour en diminuer la probabilité d'occurrence (DESROCHES, 2003);
- contrôles détectifs: ils permettent d'alerter et d'agir sur le risque lors de sa réalisation. Ils agissent, en fait, sur la probabilité et/ou l'impact;
- contrôle correctifs: ils ont pour objectif la réduction des conséquences du risque. Ils agissent essentiellement sur l'impact

Selon IFACI, PRICEWATERHOUSECOOPERS & AL. (2005; 93) «Les activités de contrôle sont constituées des politiques et procédures qui permettent de s'assure que les traitements des risques souhaités ont été effectivement mis en place. Elles sont présentes partout dans l'organisation, à tout niveau et dans toute fonction».
En plus des types de contrôles mentionnés ci-dessous, les activités de contrôle peuvent recouvrir des contrôles programmés (informatiques ou automatiques) ou manuels; généraux ou applicatifs.

Du point de vue du système d'information informatisé, les contrôles généraux recouvrent les contrôles relatifs à la gestion du système d'information, des infrastructures afférentes, de la sécurité, ainsi qu'à l'acquisition et à la maintenance des logiciels. Les

contrôles applicatifs, par contre, se préoccupent essentiellement de l'exhaustivité, l'exactitude, l'autorisation et la validité de la saisie et du traitement des données.

En tout cas, «un des objectifs majeurs des contrôles applicatifs est de prévenir l'incorporation d'erreurs au sein des systèmes, et le cas échéant de les détecter et de les corriger rapidement» (IFACI, PRICEWATERHOUSECOOPERS & AL; 2005: 98). En d'autres termes, la finalité de toute activité de contrôle reste la prévention, la détection ou la correction de la survenance des risques ou leurs conséquences négatives. Il y a donc lieu d'évaluer la capacité de ces contrôles à maîtriser les risques encourus dans l'organisation.

2.2.3.2. Evaluation des dispositifs de contrôle interne

Les dispositifs de contrôle interne mis en place doivent montrer leurs capacités de maîtrise des risques qui menacent l'organisation et son dispositif informatique. Aussi, l'évaluation de ces dispositifs de contrôle peut être effectuée sur la base des critères suivants:

- efficacité: il s'agit d'évaluer la capacité du contrôle à jouer pleinement son rôle et à atteindre les résultats pour lesquels il est mis en œuvre. Pour qu'un dispositif de contrôle interne soit jugé efficace, chacun des éléments le composant doit exister et fonctionner correctement (IFACI, PRICEWATERHOUSE & AL, 2005).
- pertinence: cela implique l'évaluation de l'utilité du contrôle en termes de coût/utilité.
- fiabilité: il s'agit d'évaluer la capacité du contrôle à fonctionner correctement de manière permanente.
- qualité: implique l'évaluation de la qualité de la conception et de la mise en œuvre.
- efficience: c'est le rapport coût/résultats/délais d'obtention des résultats qu'il convient d'évaluer.

Il convient de définir une échelle de cotation et de procéder ensuite à la cotation des dispositifs de contrôle interne existants.

2.2.3.3. Echelle de cotation des dispositifs du contrôle interne

Selon SCHICK (2010), l'échelle de cotation des dispositifs de contrôle interne existant dans l'organisation peut être définie selon les critères décrits au tableau 5 de la page suivante.

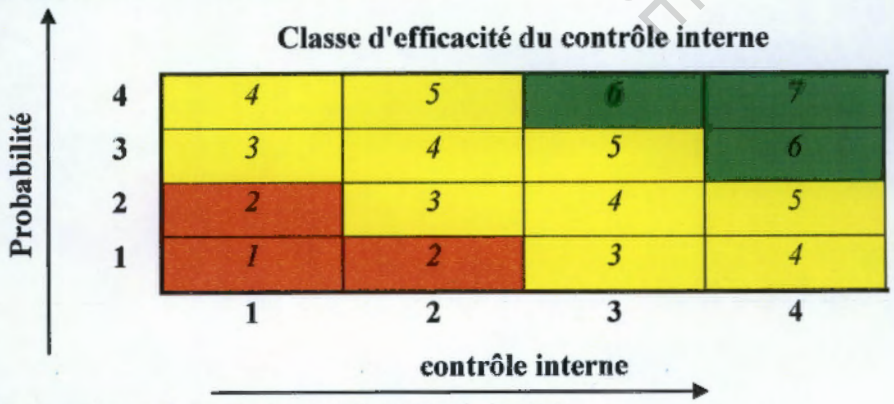
Tableau 5: Echelle de cotation du contrôle interne

Cote	critère	Définition	Efficacité du contrôle interne
1	**Non maîtrise**	Absence de pilotage de l'organisation et de formalisation des procédures, compétences insuffisantes.	**Faible**
2	**Maîtrise partielle**	Pilotage empirique, esquisse de formalisation de procédures compétences partielles.	**Modérée**
3	**Maîtrise correcte**	Pilotage existant mais perfectible, procédures existantes mais perfectibles, compétences dans le domaine.	**Elevée**
4	**Très bonne maîtrise**	Pilotage institutionnel performante, procédures rédigées, diffusées, appliquées et mises à jour régulièrement.	**Très élevée**

Source: Nous-mêmes, à partir de SCHICK (2010).

En fonction de la probabilité de survenance des risques, on peut définir trois classes correspondant à trois niveaux différents d'efficacité de contrôle interne, en termes de capacité de maîtrise des risques inhérents et/ou résiduels.

Tableau 6: Tableau d'évaluation du contrôle interne



Source: Nous-mêmes, à partir de DESROCHES (2003).

Ce résultat peut être formalisé sur un tableau traduisant le degré d'efficacité des dispositifs de maîtrise des risques mis en place. La capacité du contrôle interne à couvrir les risques peut être évaluée comme illustrée sur le tableau suivant:

Tableau 7: Matrice d'évaluation du de contrôle interne (CI)

Classe de CI	Cote	Evaluation capacité contrôle interne
1 à 2	1	faible
3 à 5	2	Modéré
6 à 7	3	Elevé

Source: Nous-mêmes, adapté de DESROCHES (2003).

2.2.4. Evaluation des risques résiduels

Le risque résiduel est le risque auquel l'entité reste exposé après la prise en compte des dispositifs de maîtrise des risques mis en ouvre. En d'autres termes c'est le risque qui subsiste après application des procédures de contrôle. Son évaluation combine celle des risques inhérents et celle du contrôle interne.

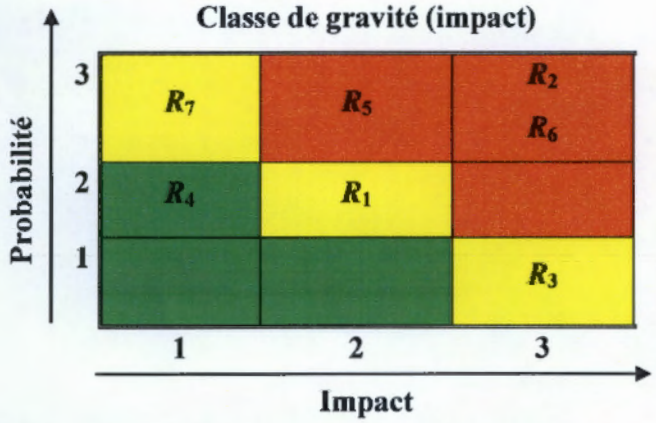
En effet, tout risque inhérent est défini par une probabilité et un impact (faible, modéré, élevé) qui, corrigé d'un dispositif de maîtrise (contrôle interne ou assurance), permet d'évaluer le risque résiduel, c'est-à-dire le risque que l'entreprise accepte de prendre, après la mise en œuvre des contrôles internes (ANGOT & AL, 2004:125).

Ce qui sous-entend que le niveau du risque résiduel doit être inférieur ou égal à celui du risque inhérent. Le risque résiduel peut également être appréhendé par l'équation suivante:

Risque Résiduel = (Impact inhérent x Probabilité inhérent) / Evaluation du contrôle interne.

Cette équation permet d'effectuer une comparaison entre le risque résiduel et le risque cible et d'établir, dans une certaine mesure, des plans d'action.

Tableau 8: Cartographie des risques résiduels



Sources: Nous-mêmes, adapté d'ANGOT & AL (2004:125).

2.2.4.1. Plan d'action de maîtrise des risques

Le plan d'action consiste à établir une panoplie des mesures formalisées et adoptées en vue du traitement des risques tels matérialisés sur la cartographie des risques.

Selon DESROCHES ((2003; 51), «la maîtrise des risques a pour but de définir et de consolider des actions permettant dans une activité donnée de rendre acceptable un évènement identifié inacceptable suite aux analyses et évaluations des risques. Plusieurs méthodes permettent de passer d'un risque inacceptable à un risque acceptable». Le risque acceptable doit correspondre au risque cible figurant sur la cartographie des risques.

2.2.4.2. Traitement des risques résiduels

Il s'agit de mettre en œuvre les mesures issues des plans d'action destinés à traiter les risques résiduels ou leurs conséquences si ces derniers se matérialisent. Le choix doit porter sur une solution ramenant le risque résiduel en deçà du seuil de tolérance souhaité par la direction (IFACI, PRICEWATERHOUSE & AL, 2005: 229).

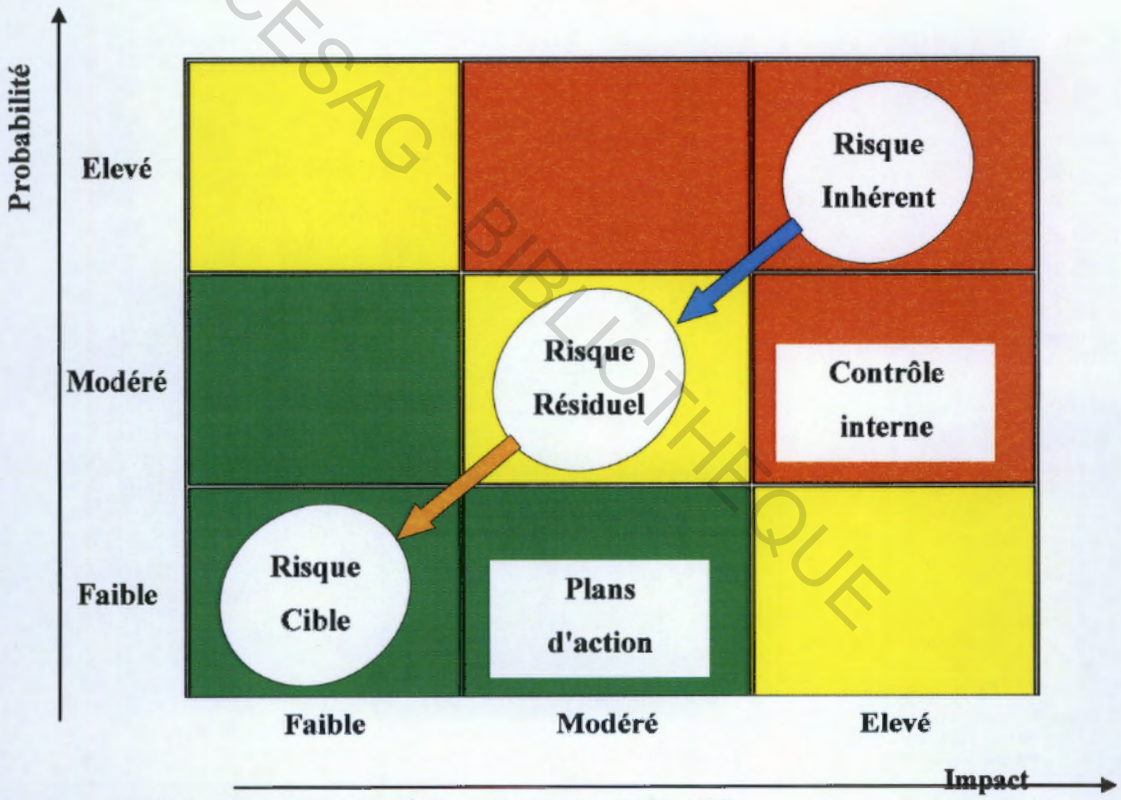
De façon pratique, les mesures à prendre sont fonction:

- de la position des risques résiduels sur la matrice des risques;
- du niveau du risque cible.

Les quatre options suivantes de gestion des risques peuvent être envisagées, à savoir:

- tolérer (ou option rétention des risques): il s'agit d'accepter les risques de niveau faible et qui offrent éventuellement de grandes opportunités;
- traiter (ou atténuer les risques): il importe, dans ce cas, de modifier les paramètres (probabilité et/ou impact) afin de le prévenir ou de le réduire en cas de manifestation effective;
- éliminer (ou terminer le risque): éviter le risque non survenu ou éliminer celui survenu par des corrections;
- transférer le risque par le biais de l'assurance.

Tableau 9: Cartographie des risques et plans d'action



Source: A partir de CHAMBAULT (in MOREAU, 2002:164)

Conclusion

Ce chapitre nous a permis de faire une description succincte du dispositif informatique, support incontournable du système d'information de l'entreprise. Toutes ces ressourees, pour être utilisées de façon optimale, doivent être organisées au travers d'une définition claire et précise du rôle et de la structure de la fonction informatique.

L'identification et l'évaluation des risques inhérents aux ressources informatiques, plus qu'une nécessité, est une contrainte pour toute organisation soucieuse de maîtriser ses risques. Dans la mesure où le système d'information et l'infrastructure qui l'accompagne sont naturellement exposés aux risques d'origines diverses (accidents, erreurs, malveillances), il est important de mettre en place un dispositif de contrôle interne efficace et adapté pour contenir ces risques ou du moins, ceux jugés inacceptables par l'organisation.
La démarche d'évaluation des risques étant décrite, il convient alors d'aborder l'approche méthodologique de sa mise en œuvre. C'est l'objet du prochain chapitre.

CHAPITRE III: METHODOLOGIE DE L'ETUDE

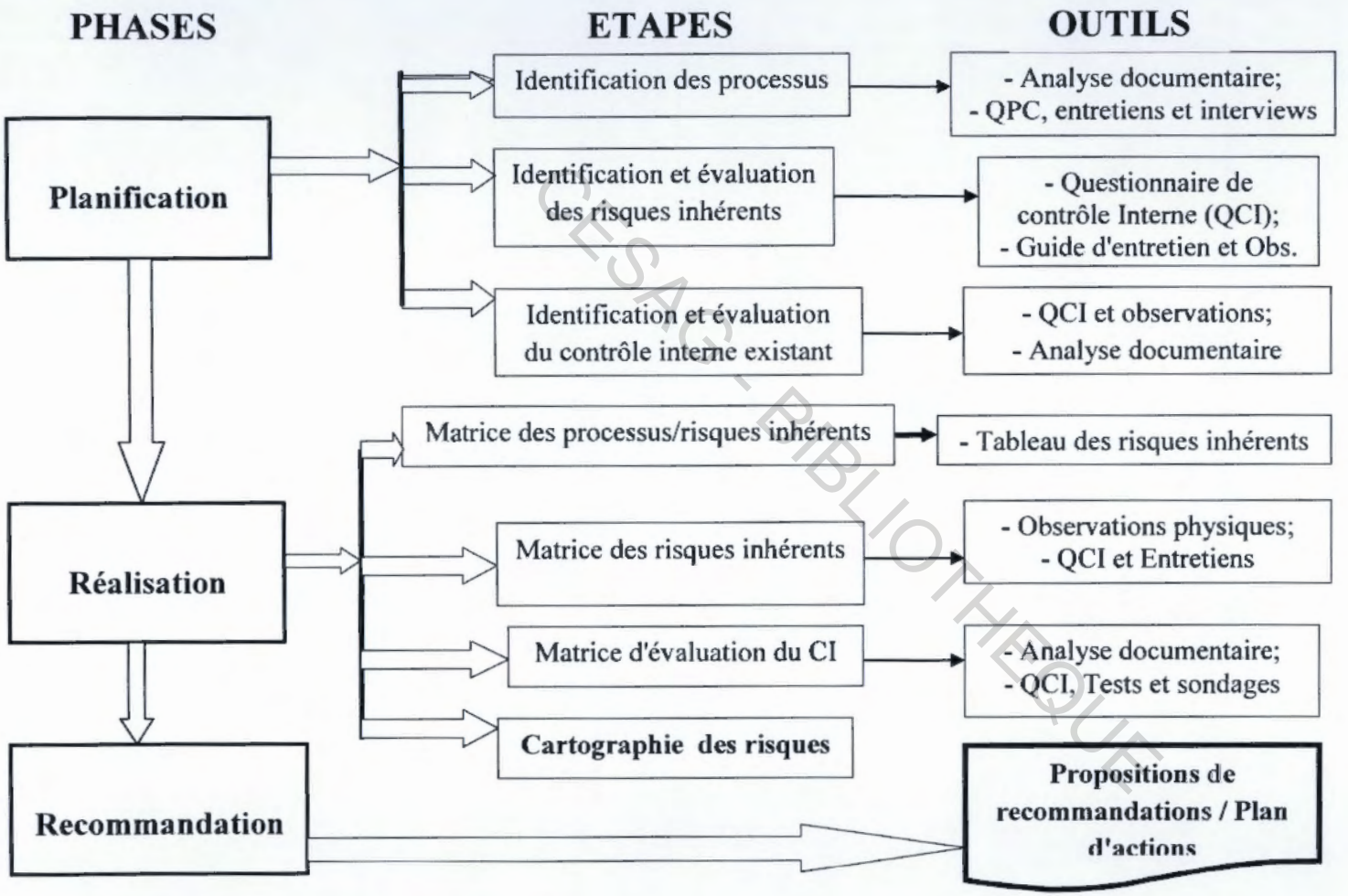
L'objet de ce chapitre est de présenter notre modèle d'analyse qui nous permettra de sous-tendre et conduire à bien la phase pratique de notre étude. En effet, il sera question de dérouler une démarche d'identification et d'évaluation des risques inhérents à l'informatique ainsi que les applications qui l'accompagnent. Pour ce faire, le choix des techniques et outils (parmi tant d'autres) adaptés au besoin de notre étude est d'une grande importance.

Dans cette perspective, la première partie consistera à présenter notre modèle d'analyse et la seconde sera consacrée à la description succincte des outils de collecte et d'analyse de données utiles à l'évaluation des risques.

3.1. Modèle d'analyse

Selon JIMENEZ & al (2007 :55) « un modèle est une représentation schématique de tout ou partie de l'entreprise dans un langage de représentation approprié ».
En ce qui nous concerne, notre modèle traduit ici notre démarche d'identification et d'évaluation des risques dans l'optique d'élaboration d'une cartographie, outil de gestion des risques et des ressources. Cette démarche est axée sur trois phases et sept étapes décrites sur la figure 4 de la page suivante.

Figure 4:Modèle d'analyse



Source: Nous-mêmes

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

L'utilisation de certaines techniques et outils de collecte et d'analyse des données s'avère très utile dans la mesure où ils permettent d'organiser et d'orienter la démarche pour la réalisation des travaux d'identification et d'évaluation des risques. En fait, les techniques sur lesquelles nous portons nos choix ne constituent pas des normes de travail à proprement parler mais plutôt des moyens et outils qui permettent de conduire au mieux l'évaluation des risques et du dispositif de contrôle interne. Ces outils peuvent être des outils de collecte d'information, d'analyse des données ou encore de diagnostic. Ils peuvent être utilisés séparément ou en les combinant pour obtenir de meilleurs résultats.

Nous présentons ci-dessous, quelques techniques sélectionnées parmi tant d'autres et qui découlent de certaines approches méthodologiques de conduite des travaux d'évaluation des risques et du contrôle interne.

3.2.1. L'analyse documentaire

L'analyse documentaire consiste à l'exploitation des documents de l'organisation faisant objet de l'étude. Il s'agit de consulter et de synthétiser les informations contenues dans les documents obtenus afin d'en tirer, un tant soit peu, une connaissance générale ou approfondie de l'entité étudiée. C'est une technique couramment utilisée lors de la prise de connaissance des domaines, objets de l'étude. L'analyse documentaire se fera tout au long du déroulement de la phase pratique de notre étude.

3.2.2. Le tableau des risques

Le tableau des risques constitue l'outil de référence qui permet d'une part, de définir le champ et les limites d'investigations et d'autre part, de structurer la présentation des analyses et conclusion, notamment pour renseigner ce qui relève de(s) constat(s), la ou les causes des faits constatés ainsi que leurs conséquences. (SCHICK & AL, 2010).

Ce tableau découpe l'activité (la fonction ou le processus), objet de l'étude, en tâches élémentaires et permet d'associer à chaque tâche, les risques susceptibles d'empêcher la réalisation des objectifs ainsi que les bonnes pratiques de contrôle interne à mettre en œuvre.

En fonction du degré d'affinement de l'analyse, le tableau des risques comportera cinq colonnes ou plus, si nécessaire. Le tableau des risques se remplit de gauche à droite, étant entendu que ce remplissage est le support d'un raisonnement où chaque colonne est affinée par la colonne suivante, et inversement chaque colonne se déduit de la colonne suivante, comme indiqué sur le tableau ci-dessous.

Tableau 10: Tableau des risques

Finalités /objectifs de CI ...du stade/ opération/ élément	**Empêchement** Risque que la finalité ne soit atteinte	**Points de contrôle** Etapes clés du CI observables	**Impact / risque** Si étape clé défaillante/déficiente	**Bonnes pratiques de CI** Moyens, ressources,...
"Etre sûr que telle finalité de l'organisation sera atteinte, que tel aspect/ étape du processus est sous contrôle et maîtrisé"	**Scénario de risque:** Que peut-il se passer?	Exemples de critères de contrôle: Exactitude Exhaustivité Autorisation Délai Suivi	Image Ethique Financier ...	Adoptées Adaptées Disponibles Performantes
1	**2**	**3**	**4**	**5**

Source: SCHICK (2010: 108).

3.2.3. Interview

L'interview est une technique de recueil d'informations qui permet d'expliquer et de commenter le déroulement des opérations afférentes à un processus. Elle permet d'appréhender les différents processus de l'organisation en posant des questions aux personnes impliquées dans le domaine étudié. L'interview aide à recueillir de l'information afin de comprendre, pour chaque opération réalisée: les objectifs poursuivis, la nature des tâches exécutées, les documents utilisés, les difficultés rencontrés et ainsi identifier les risques potentiels. Elle sert aussi dans certains cas pour délimiter le champ et les objectifs.

3.2.4. Questionnaires

Selon SHICK & AL (2010), un questionnaire est une liste de questions auxquelles on doit répondre par écrit. Les réponses sont généralement reportées par la personne administrant le questionnaire, on parle alors "d'administration indirecte", mais il arrive que l'interrogé remplisse lui-même le questionnaire, on parle dans ce cas "d'administration directe".

Le questionnaire peut être structuré sous forme de questions à choix multiples (QCM) ou de questions ouvertes (Q.O) pour lesquelles le choix de réponses n'est pas limité. Les questionnaires sont utilisés :

- d'abord comme étant un outil d'analyse de l'activité étudiée en vue d'identifier les points forts et les points faibles en se basant sur les questions posées et les réponses recueillies;
- ensuite comme outil d'interview, à travers les questions préparées pour orienter et guider l'interview.

Il existe deux sortes de questionnaires, à savoir:

- le questionnaire de prise de connaissance (QPC), intervenant lors de la phase de préparation de l'étude;
- le questionnaire de contrôle interne (QCI) intervenant pendant la phase de réalisation.

Le questionnaire de prise de connaissance permet de récapituler les questions importantes dont la réponse doit être connue si on veut avoir une bonne compréhension du domaine étudié. C'est un moyen efficace pour organiser la réflexion et surtout pour:

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

Le questionnaire de contrôle interne est un véritable outil méthodologique permettant d'identifier:

- les contrôles internes mis en place pour se protéger contre les risques et erreurs potentiels;
- les objectifs d'évaluation pour vérifier qu'ils sont respectés.

L'élaboration du questionnaire de contrôle interne doit aider à répondre aux cinq questions fondamentales qui regroupent l'ensemble des interrogations concernant les points de contrôle et qui permettent de couvrir tous les aspects: *Qui? - Quoi? - Où? - Quand? - Comment?*

3.2.5. Observation physique

Selon SCHICK & AL. (2010), l'observation physique est la constatation de la réalité instantanée de l'existence et du fonctionnement d'un phénomène (un processus, une transaction, un site, un bien, des documents, des comportements, ...).

L'observation physique peut s'appliquer pour:

- les biens immobilisés tangibles tels que les terrains, immeubles, aménagements, ...;
- les biens mobiliers tangibles: matériels et équipements de toute nature;
- les documents représentatifs de droits ou dettes,...:
- les processus matériels de contrôle et de protection des actifs;
- les éléments incorporels représentatifs de la position de l'entité concernée.

L'observation physique revêt deux formes, à savoir:

- l'observation directe qui consiste essentiellement en la vérification détaillée et visuelle d'une structure, fonction, processus, procédure donnés par rapport au processus en vigueur. Ce processus devant porter les mêmes marques d'identification que sur le bien en question. Elle doit permettre de porter un jugement ou avis sur l'état physique du bien à l'instant de l'observation.
- l'observation physique indirecte qui consiste à vérifier l'existence d'un bien au travers de documents authentiques au sens juridique du terme, ou de documents émis par des tiers liés au sujet par des relations juridiques précises et strictes.

En tout état de cause, l'observation physique sera privilégiée à la phase pratique dans la mesure où c'est une technique qui présente les garanties les plus solides, en ce sens qu'il n'est rien de plus fiable que le phénomène observé directement par la personne intéressée.

3.2.6. Sondages statistiques

Selon LEMANT (1991), le sondage statistique est une technique qui permet, à partir d'un échantillon prélevé aléatoirement dans une population de référence, d'extrapoler à la

population les observations effectuées sur un échantillon, avec une certitude spécifiée et une précision désirée.

La méthode des sondages statistiques peut se faire selon quatre étapes (non détaillées) citées ci-dessous:

- la préparation physique du sondage;
- le prélèvement de l'échantillon;
- l'observation des faits et calculs;
- la formulation des résultats.

Cette technique est particulièrement intéressante lors du déroulement de la phase pratique pour effectuer certaines vérifications, en ce sens qu'elle permet d'obtenir des éléments probants pour étayer les constats de dysfonctionnements qui pourraient être relevés. Nous pourrons éventuellement faire appel à cette technique pour valider les réponses, réputées positives, des questionnaires de contrôle interne que nous aurons mis en œuvre.

Conclusion

Ce chapitre a permis de manifester succinctement la démarche référentielle que nous entendons dérouler au cours de la phase pratique de notre étude. Mais il nous aura surtout donné l'occasion de décliner les différents outils plus ou moins adaptés à mettre en œuvre pour la réalisation de l'évaluation des risques informatiques et de son contrôle interne.

Ce chapitre marque donc la fin de notre revue de littérature sur l'évaluation des risques opérationnels informatiques et le passage à la phase pratique de notre étude.

CONCLUSION DE LA PREMIERE PARTIE

La revue de la littérature sur les risques opérationnels informatiques a permis d'étudier les aspects représentant les enjeux du dispositif informatique, en termes de risques potentiels. Nous avons également présenté, au cours de cette revue notre modèle d'analyse en vue de l'identification et l'évaluation de ces risques.

L'inhérence des risques informatiques, plus qu'une nécessité, doit être une préoccupation majeure des responsables concernés de la COTONTCHAD dont l'activité principale (commercialisation de la fibre coton) est tributaire de l'environnement du commerce mondial. De ce fait, elle se trouve, évidemment, exposée aux enjeux de la mondialisation qui accentuent les risques menaçant son système d'information en général, ouvert sur l'extérieur. Pour cela, il est important pour les responsables de cette société de bien connaitre les risques qui menacent les systèmes d'information et informatique. Cela passe par l'identification et l'évaluation de ces risques relatifs à ce dispositif.

De cette connaissance découleront les mesures appropriées que pourrait prendre la société pour les traiter et assurer un niveau satisfaisant de sécurité informatique, gage de performance de son système d'information tout entier.

DEUXIEME PARTIE: CADRE PRATIQUE

INTRODUCTION DE LA DEUXIEME PARTIE

La gestion de l'organisation et l'atteinte de ses objectifs implique que l'information irrigue chaque niveau de la structure organisationnelle afin d'identifier, évaluer et répondre aux risques. L'informatique, en tant que support incontournable du système d'information de l'entreprise, est exposée à de nombreux risques inhérents et des nouveaux risques engendrés par l'ouverture de celle-ci sur le monde extérieur. Il convient donc d'identifier, évaluer et gérer au mieux ces risques liés à l'utilisation des systèmes d'information informatisés afin que la fiabilité, la disponibilité, l'intégrité, la confidentialité et, de façon générale, la sécurité des informations produites par l'entreprise soient garanties. De cette évaluation des risques découleront les mesures de sécurité à prendre pour veiller sur les actifs de la société afin de les protéger au mieux.

La COTONTCHAD, dont les activités sont cycliques, saisonnières et tributaires de l'évolution des cours du marché mondial de coton fibre, est l'objet d'importants risques. Ses infrastructures et applications informatiques n'y échappent pas. Dans ce souci, il convient d'effectuer une évaluation des risques opérationnels informatiques liés à ces ressources afin de dégager une cartographie qui sera l'outil de gestion de ces risques. C'est l'objet principal de cette partie.

Dans cette perspective, nous présenterons d'abord la COTONTCHAD dans un bref aperçu de ses caractéristiques et son organisation interne (chapitre 4). Nous procéderons ensuite à un état des lieux de l'environnement de la fonction informatique et de ses processus (chapitre 5). Enfin, nous déclinerons les travaux d'évaluation des risques pour dégager les forces et faiblesses de l'entité en charge de la fonction informatique. Nous proposerons quelques recommandations susceptibles d'être mises en œuvre pour améliorer, si possible, la situation en termes de fiabilité, d'efficacité et de performance (chapitre 6).

CHAPITRE IV: LA SOCIETE COTONNIERE DU TCHAD "COTONTCHAD"

Introduction

La société cotonnière du Tchad "COTONTCHAD" a été créée le 29 Octobre 1971 à la suite d'un protocole d'accord signé le 21 Avril 1971 entre le gouvernement tchadien et ses partenaires qui sont:

- COTONFRAN (Compagnie Cotonnière Française);
- GEOCOTON (ex DAGRIS: Société de Développement des Agro-industries du Sud);
- ECOBANK (ex BIAT: Banque Internationale pour l'Afrique au Tchad);
- Société Générale Tchad (SGT), ex BTCD (Banque Tchadienne des Crédits et Dépôts).

La COTONTCHAD est une Société anonyme (SA) d'économie mixte, au capital social de 4,256 Milliards (4.256.000.000) FCFA divisé en 200.000 actions de 21.280 FCFA de valeur nominale chacune. La composition de ce capital est la suivante:

Tableau 11: composition du capital de la COTONTCHAD

Actionnaire	Nbre action	Valeur	% Capital	Montant (FCFA)
ETAT TCHADIEN	150 000	21 280	75,00%	3 192 000 000
GEOCOTON	38 000	21 280	19,00%	808 640 000
SGT	9 000	21 280	4,50%	191 520 000
ECOBANK	3 000	21 280	1,50%	63 840 000
TOTAL	**200 000**	**21 280**	**100,00%**	**4 256 000 000**

Source: Etas financiers au 31 Décembre 2010, COTONTCHAD (2011: 17).

Pour faciliter son développement et assurer la pérennité de ses activités, la COTONTCHAD a pris des participations dans le capital d'autres sociétés tchadiennes et étrangères. Le pourcentage de ses prises de participation est récapitulé sur le tableau 4 de la page suivante:

Tableau 12: prise de participation de la COTONTCHAD dans d'autres sociétés

SOCIETES	PARTICIPATION COTONTCHAD (en %)	Montant participation
SIMAT (Tchad)	65,00%	30.100.000
STAT (Tchad)	50,00%	140.550.000
STAR National (Tchad)	26,89%	132.952.000
SCIEP (Cameroun)	40,28%	145.000.000
SOSEA (France)	10,00%	3.500.000
COPACO (France)	0,41%	35.450.000
TOTAL Participations		**487.552.000**

Source: Etas financiers au 31 Décembre 2010, COTONTCHAD (2011: 18).

4.1. Présentation de la COTONTCHAD

Cette section permettra d'évoquer brièvement l'historique de la COTONTCHAD, ses missions et objectifs, de faire un aperçu général de son organisation interne mais aussi et surtout de parler de ses activités afin de comprendre globalement le rôle qu'elle joue sur l'échiquier économique du Tchad.

4.1.1. Historique

Introduit au Tchad vers l'année 1921, la culture du coton s'imposa véritablement autour des années 1926 – 1928 et gagna progressivement toute la zone sud du Tchad, appelée aussi zone méridionale. L'installation de la société franco-belge COTONFRAN vers l'année 1934 a été l'occasion pour celle-ci de créer dans la plupart des régions dites méridionales des usines d'égrenages implantées dans les grandes villes. Le coton était devenu, dès lors, un véritable enjeu économique et commercial important de cette société coloniale, très satisfaite du développement spectaculaire de la culture du coton au Tchad.

Plus d'une quarantaine d'années plus tard, la société cotonnière coloniale COTONFRANC devait cesser ses activités au Tchad. Un protocole d'accord fut alors signé entre la République du Tchad, ses partenaires et COTONFRANC. La signature de ce protocole d'accord a donné naissance le 29 octobre 1971 à la société cotonnière du Tchad

dénommée "COTONTCHAD". Son capital social à la création était fixé 600 Millions de francs (600.000.000.FCFA) divisé en soixante mille (60.000) actions de valeur nominale de dix mille franc (10.000 FCFA) chacune. La société ainsi créée avait, selon ses statuts, pour objet social:

- l'achat du coton graine, son égrenage et la commercialisation du coton et des sous-produits du coton;
- la participation à toutes opérations de développement agricole du Tchad, tant sur le plan industriel et commercial que sur celui de la production;
- et, généralement, toutes opérations de quelque nature qu'elles soient, se rattachant directement ou indirectement à l'objet social et susceptible d'en faciliter la réalisation.

4.1.2. Mission et objectifs de la COTONTCHAD

Selon les termes des articles 1 et 2 du décret N° 61 /PR/MEC/85 du 12 septembre 1985, approuvant le renouvellement de la convention d'établissement passée entre le Tchad et la COTONTCHAD, le gouvernement de la République du Tchad donne mission à la société cotonnière du Tchad "COTONTCHAD" qui accepte:

- d'assurer en exclusivité la commercialisation de coton (achat et transport coton graine, égrenage, emballage, vente de coton fibre et sous-produit de coton) produit au Tchad;
- de participer au développement de la production et de la productivité agricoles en liaison avec les organisations et les charges de production et de la promotion rurale;
- de s'engager à acheter tout le coton graine qui sera apporté individuellement par les producteurs sur les marchés ou livré par les groupements des producteurs.

Toutes les activités menées par la COTONTCHAD doivent donc concourir à l'accomplissement de cette mission ou de ces objectifs qui lui sont assignés.

4.1.3. Activités de la COTONTCHAD

L'activité principale de la COTONTCHAD, consiste à l'achat du coton graine aux producteurs, son transport, son égrenage et la commercialisation de la fibre et sous-produit du coton. La COTONTCHAD s'implique aussi dans toutes les opérations de développement agricole du Tchad tant sur le plan industriel et commercial que celui de la production.

Les activités d'égrenage et de mise en balle de la fibre de coton se déroulent essentiellement dans les neuf (09) usines qui constituent l'essentiel de l'outil industriel de la COTONTCHAD. Ces usines sont toutes implantées au sud, dans les grandes villes de la zone méridionale, où est produit le coton graine, à savoir (de l'Est à l'Ouest), les usines de KYABE, SARH, KOUMRA, DOBA, MOUNDOU, KELO, PALA, GOUNOU-GAYA et LERE. Ces usines peuvent ensemble égrener plus de deux cent cinquante mille tonnes (250.000 T) de coton graine par an, dans des conditions de bon fonctionnement des machines.

L'Annexe 1.1 de la page 100, donne un aperçu global des caractéristiques de chaque usine ainsi que la capacité réelle de production de celle-ci. Compte tenu des difficultés notamment financières que connait la COTONTCHAD depuis quelques années, trois des neuf usines sont mises sous "cocon" il y a trois ans mais doivent bientôt bénéficier d'un vaste programme d'investissement pour leur réhabilitation. Il s'agit des usines de Kyabé dont la capacité annuelle de production est estimée à 9.000 Tonnes de coton graine, celles de Doba et Gounou-Gaya dont les capacités annuelles d'égrenage coton graine sont de 16.800 Tonnes chacune.

Pour assurer une bonne production cotonnière par les paysans et partant, de la fibre (cf. Annexe 1.2, page 100), la COTONTCHAD met gracieusement à la disposition des producteurs des variétés de semences produites dans certaines de ses usines. Du point de vue commercial, elle achète des intrants agricoles (engrais, insecticides, piles, appareils de traitement cotonnier, balances) qu'elle revend à crédit aux paysans producteurs et procède au recouvrement lors de la commercialisation du coton graine. Cette activité commerciale, bien que procurant d'importantes ressources au côté de celles générées par la vente de coton fibre et ses sous-produits (huile et tourteau), n'est pas sans risque car la COTONTCHAD se retrouve actuellement avec des arriérés cumulés de plus de quatre milliards non recouvrés, selon la Direction de Production Cotonnière (DPC).

La fibre produite est destinée à l'exportation et commercialisée sur le marché international. Celle déclarée non exportable est vendue sur le marché local, au Tchad ou dans les pays voisins, en particulier au Nigeria.

La COTONTCHAD dispose d'une unité industrielle de production de savon, d'huile et de tourteau à partir des graines de coton triturées. La production de tourteau est destinée à

l'alimentation des bétails. Depuis quelques années le savon n'est plus produit du fait de manque de la principale matière première entrant dans sa fabrication à savoir l'acide gras de palme importé et devenu depuis lors trop cher sur le mareché international ainsi que les autres composants. Seuls l'huile et le tourteau sont produits pour les besoins du marché intérieur.

4.1.4. Impact socio-économique des activités de la COTONTCHAD

Avant l'ère pétrolière, la COTONTCHAD était le plus grand employeur, juste derrière l'Etat tchadien. En pleine campagne cotonnière la société pouvait employer plus de 2.000 employés (permanents et saisonniers). A titre d'illustration, l'Annexe 1.3 présente l'évolution de l'effectif du personnel durant les cinq dernières années. On constate que l'effectif du personnel a fortement diminué à partir de la campagne cotonnière 2008/2009. Cette situation est consécutive à la fermeture des trois usines intervenue du fait des difficultés financières persistantes que connait la société.

La masse salariale versée à ses employés est d'environ 4 Milliards de franc par an (cf. Annexe 1.3) représentant en moyenne 12,18% du chiffre d'affaires (CA) annuel global durant les cinq dernières années. Les chiffres d'affaires et les résultats nets figurent à l'Annexe 1.4.

Sur le plan socio-économique, plus de trois millions (3.000.000) de tchadiens tirent l'essentiel de leurs revenus directement ou indirectement des activités de la COTONTCHAD. Il s'agit au premier plan d'environ deux cent mille (200.000) producteurs repartis au sein de quelques trois mille (3.000) Associations Villageoises (**AV**) qui bénéficient de plus de 40 Milliards de franc versés par la COTONTCHAD au titre d'achat coton graine durant une campagne.

Les partenaires de la COTONTCHAD, tels que les commerçants, fournisseurs divers, transporteurs, et autres prestataires de services réalisent d'importants chiffres d'affaires avec cette société qui demeure leur principal pourvoyeur de revenu, du moins dans la zone méridionale du pays. Il en va de même des autres acteurs impliqués dans la filière coton qui tirent une partie de leurs revenus au travers des transactions effectuées avec la COTONTCHAD.

4.2. Organisation interne de la COTONTCHAD

L'organisation interne (hiérarchique et fonctionnelle) de la COTONTCHAD est traduite par son organigramme figurant à l'Annexe 2. Cette organisation s'appuie sur une structure dirigeante composée comme suit:

- L'Assemblée Générale des actionnaires ;
- Le Conseil d'Administration (CA);
- La Présidence Direction Générale (PDG).

Les unités opérationnelles rattachées à la Présidence-Direction Générale (PDG) et à la Direction Générale adjointe sont composées de huit directions et deux départements qui sont:

- La Direction Administrative et des Ressources Humaines (DARH);
- La Direction de Production Cotonnière (DPC);
- La Direction Technique des Usines (DTU);
- La Direction Financière et Comptable (DFC);
- La Direction Commerciale et marketing (DCM);
- La Direction Logistique, du Parc et Matériel (DLPM);
- La Direction de Contrôle de Gestion et de l'Audit Interne (DCGAI), structure à laquelle nous appartenons;
- La Direction de l'Huilerie Savonnerie (DHS);
- Le Département Approvisionnement et Magasin Général (DAMG);
- Le Département Informatique (D.I).

Ce dernier département a été le lieu de notre stage et étude. Nous parlerons particulièrement de cette entité au prochain chapitre.

Conclusion

Ce chapitre nous a permis de faire une brève présentation de la société COTONTCHAD et sa structure organisationnelle. On comprend, de façon générale, que c'est une entreprise géante, aussi complexe par ses structures que par son fonctionnement, mais dotée d'un important poids dans le tissu économique du Tchad par l'emploi et les redistributions des revenus qu'elle réalise.

CHAPITRE V: DESCRIPTION DES APPLICATIONS INFORMATIQUES

Il sera procédé dans ce chapitre à la présentation de la structure en charge de l'informatique de la COTONTCHAD, son organisation interne ainsi que la description de son système informatique et les applications opérationnelles qui accompagnent ce système.

Dans le même ordre d'idée, nous procéderons à l'identification des processus informatiques existants et éventuellement à leur découpage en sous-processus à retenir pour l'évaluation des risques inhérents, réputés majeurs, dans le but de dégager les forces et faiblesses du système qui fonctionne actuellement. Cette démarche aura pour finalité de déboucher sur l'établissement d'un tableau des risques ou d'une cartographie des risques pouvant permettre d'envisager des mesures susceptibles d'améliorées les faiblesses identifiées.

5.1. Prise de connaissance de la fonction informatique de la COTONTCHAD

La prise de connaissance générale est une étape très importante car d'elle dépend la bonne compréhension des missions et activités de la fonction informatique et des processus gérées par celle-ci. Mais avant tout, il convient de faire une brève historique de cette fonction, son évolution et celle de son système informatique.

5.1.1. Historique

La nécessité de créer un service informatique s'était fait ressentir dès l'année 1984 où la Direction Générale était encore établie à N'Ndjamena. Le service informatique fut crée cette année-là et avait pour principales missions:

- l'étude et le développement informatiques;
- la maintenance des équipements et applications informatiques.

Le service ainsi crée, était équipé d'un mini ordinateur (mini système) appelé DPS 4 et quelques matériels informatiques d'accompagnement. Les personnel était composé de:

- trois (03) analystes-programmeurs;

- deux (02) techniciens de maintenance.

Deux applications à savoir la PAIE et les IMMOBILISATIONS (IMMO) ont été acquises à cette époque et une application en COMPTABILITE a été développée en interne par les analystes programmeurs. Ce qui avait permis de lancer concrètement les activités.

Les différentes phases d'évolution de ce service peuvent être résumées comme suit:

- 1986: développement d'une application en gestion des stocks;
- 1992: élaboration du Schéma Directeur Informatique (SDI) ayant pour objectif de définir les axes d'évolution du système d'information nécessaire. Il devait aussi permettre de définir les priorités et lister les projets à réaliser, mais non mis en œuvre;
- 1994: rattachement du service informatique à la Direction du Contrôle de Gestion et de l'Audit Interne et détachement de la section maintenance rattachée un an plus tôt au service électrique de la Direction d'Exploitation (DE);
- 1996: introduction de la micro informatique entrainant le recrutement de deux informaticiens mais également le départ de deux anciens agents. Ce qui maintenait l'effectif du personnel à cinq agents. Dans le même temps, il avait été développé une application de gestion du personnel et une autre application de gestion des intrants sous le logiciel FOX PRO. Des développements des programmes de suivi de la production fibre et balles coton et de leur évacuation ont également été effectués.
- 2001: les programmes de gestion des stocks développés sont basculés sous VISUAL FOX PRO à partir de l'existant et migrés sous les micros ordinateurs;
- 2005: installation de l'internet à travers l'implantation des VSAT;
- 2010: migration des applications PAIE, COMPTA, IMMO vers SAGE (édition pilotée) sous SQL-SERVEUR (base de données), application acquise auprès d'un prestataire en externe et installée sur des micros ordinateurs des services utilisateurs de directions opérationnelles. Dans le même temps, on a procédé à la décentralisation des saisies des données et opérations qui étaient auparavant effectuées en pool au niveau de la Direction Financière et Comptable (DFC), en ce sens que chaque agent est directement responsable de saisie de ses données et opérations. Le service informatique ne s'occupant que de l'intégration de ces données dans celles de la comptabilité. C'est également au cours de l'année 2010 qu'il a été implanté des VSAT à N'djamena et en 2012 toutes les usines ont été dotées de cet outil de communication.

A la fin de l'année 2010, le service informatique avait été détaché de la Direction du contrôle de Gestion de l'Audit Interne et Informatique (DCGAI) pour être érigé en Département de l'Informatique (DI), structure autonome, directement rattachée à la Direction générale. De ce fait, elle devient l'interlocutrice directe de celle-ci. Le Chef de Service informatique est, dès lors, nommé Chef de Département Informatique (CDI).

5.1.2. Mission et activités du Département Informatique (DI)

La mission et les activités du département informatiques ont été renforcées dès son passage du stade de service au statut de département.

5.1.2.1. Mission

Crée en 2010 par décision de la Direction Générale, le Département Informatique a pour missions principales:

- études, développement et exploitation des ressources informatiques afin de mettre à la disposition des utilisateurs des outils opérationnels;
- maintenance des applications et programmes informatiques;
- gestion des réseaux, télécommunications et assistance (formation, conseil) aux utilisateurs.

Le Département Informatique est directement rattaché à la Direction Générale. Son responsable, le Chef de département, a rang de Directeur Adjoint et est membre du Comité de Direction (CODIR). Cette responsabilité lui permet d'être informé en toute circonstance de toutes les grandes décisions influençant la stratégie de la société ou ses choix.

5.1.2.2. Activités

Les activités du Département Informatique (DI) sont essentiellement celles découlant de la mission qui lui est assignée. Il s'agit de:

- mener des études et développer des applications répondant aux besoins de la société;
- lancer des opérations de tests et jeux d'essaie;
- mettre en place les applications développées ou acquises;
- maintenir le système réseau et assister les utilisateurs (petits dépannages);

- veiller au bon fonctionnement des équipements informatiques et du réseau;
- maintenir et faire évoluer les applications développées en interne ou acquises et/ou modifier les programmes en fonctionnement;
- former et conseiller les utilisateurs dans tous les domaines informatiques;
- trouver les solutions informatiques répondant aux besoins des utilisateurs
- veiller au bon fonctionnement de l'internet;
- élaborer les budgets de fonctionnement et d'investissement de département;
- rédiger les cahiers de charges pour les contrats d'acquisition des équipements et des prestations des services informatiques.
- gérer l'ensemble du parc informatique de la COTONTCHAD.

5.2. Organisation interne du département

L'organisation interne du département n'est pas formelle en ce sens qu'il n'existe pas d'organigramme établi et définissant clairement le rôle de chaque agent et les limites des ses tâches et responsabilités. Il n'existe pas non plus de services ou section organisés en domaines d'activités sous la responsabilité du département et obéissant à la séparation des fonctions ou tâches pour une bonne maîtrise des activités en termes de pilotage et performance. De plus, l'effectif actuel du personnel du département est insuffisant en nombre et compétence pour couvrir l'ensemble des domaines de services délivrés par la fonction informatique.

L'effectif actuel du personnel du département informatique est composé de trois personnes à savoir:

- le Chef de département informatique qui est un agent cadre ayant 22 ans d'ancienneté et d'expérience professionnelle dans le métier au sein de la COTONTCHAD. Comme tout responsable d'une direction, il a la charge d'organiser, de planifier, de superviser et de contrôler ou, bref, de piloter les activités du département informatique.
- un analyste programmeur, agent de maîtrise, ayant 9 ans d'ancienneté à la COTONTCHAD. Il a pour principales tâches de maintenir en bon état de fonctionnement les applications et programmes informatiques, d'effectuer des corrections sur des programmes et éventuellement de procéder aux modifications de ces programmes à la demande des utilisateurs.
- un agent de maintenance réseau, recruté il y a un an.

- il s'occupe essentiellement de l'exploitation du réseau, des sauvegardes des données, des configurations et des installations d'anti-virus, bref, de la bureautique des usagers.

5.3. Fonctionnement du Département Informatique

Il n'existe pas de manuel décrivant les méthodes et procédures de fonctionnement ou de travail du département. Il n'y a pas, non plus en pratique, des méthodes et procédures de travail adoptées. Cependant, le travail est organisé quotidiennement par le responsable du département sur la base du recensement des besoins et problèmes éprouvés par les utilisateurs, de leurs attentes ou des résultats et solutions attendus des problèmes identifiés.

A partir des problèmes posés par les utilisateurs ou par la société en général, le responsable du département procède à la répartition d'un certain nombre de tâches relatives à ces préoccupations à ces deux agents. Il oriente l'exécution de ces tâches et les méthodes de travail à utiliser pour parvenir aux résultats attendus.

A la fin des travaux, il procède au contrôle des résultats obtenus et éventuellement procède à leur validation. A la limite, le Chef de Département fait presque tout, du moins dans certaines circonstances, du fait même de l'absence d'organisation du département en services ou section séparés.

5.4. Diagnostic de l'existant

Cette démarche permettra, à partir d'un constat, de décrire ou détailler le fonctionnement actuel du système informatique et d'information de la société. Elle nous permettra de diagnostiquer les forces et faiblesses, mais aussi de définir les règles d'intégration et d'échange des informations entres les diverses entités de la société.

Les points à aborder lors de cette démarche sont essentiellement les suivants:

- inventaires des ressources informatiques (matériels et logiciels);
- identification des processus clés et du schéma fonctionnel des applicatifs existants,
- cartographie applicative et de ses interfaces;
- principaux volumes traités.
- relation avec les utilisateurs.

5.4.1. Les ressources informatiques de la COTONTCHAD

Le parc informatique de la COTONTCHAD est essentiellement constitué des micros ordinateurs, des imprimantes, des matériels de partage en réseau (Switchs, routeurs, pare-feu) et de sécurité (onduleurs, pare-feu). Le recensement de ce parc et l'évaluation de son état de fonctionnement portant uniquement sur les micros ordinateurs et imprimantes est consigné sur un récapitulatif figurant en Annexe 3.

5.4.1.1. Les ressources matérielles du département informatique

Les ressources matérielles du département et autres équipements informatiques accompagnant celles-ci; servant de support aux processus métiers sont essentiellement constitués des éléments figurant en **Annexe 3** (annexe 3.2).

Ces ressources telles qu'identifiées et décrites dans leurs rôles sont les moyens techniques dont dispose le département pour soutenir le système d'information de la COTONTCHAD, du moins, en ce qui concerne sa partie automatisée.

5.4.1.2. Les logiciels et applications informatiques

En dehors des logiciels standards d'exploitation (WINDOWS...), de calcul (tableurs) ou de traitement de texte, les applications informatiques de la société sont soit acquises (progiciels ou standards) soit développées en interne (solutions spécifiques). Dans les deux cas, c'est le département informatique qui s'occupe de la maintenance et éventuellement des modifications de ces applications ainsi que de leur évolution. Le tableau 5 de la page suivante donne un aperçu de la cartographie des principales applications existantes.

Les autres applications, actuellement opérationnelles, sont:

- "**Gestion Production-Evacuation**": développée en 1996, cette application permet le suivi de l'approvisionnement en coton graine, son transport, la production de balles fibre et leur évacuation au sous-transit de N'gaoundéré (CAMEROUN).
- "**Classement**": application basée sur SQL-Serveur et mise en production en 1997, elle permet de saisir les résultats du classement par qualité de coton, balle par balle.

- Cette saisie, par rapprochement avec la saisie de la production des usines permet de détecter des anomalies commises dans les usines. Ainsi toutes les qualités des balles de coton sont connues, ce qui limite les erreurs à l'évacuation.
- **"Direction Technique des usines"**: (1998) le progiciel permet de saisir quotidiennement et par usine, les entrées coton graine, les résultats d'égrenage, le coton payé.il permet également d'éditer, après consolidation des données de **"Gestion "Production-Evacuation"** des usines les informations telles que le coton graine entrée, évacué, le nombre de balles de fibre produite, classées et évacuées ainsi que les stocks de fibre et graines de coton.

Tableau 13: cartographie des principales applications

APPLICATION	Type	Editeur/Prestataire	Date mise en service	Principales fonctionnalités
PAIE V19	Progiciel	Sage Edition Pilote	**2010**	Gestion des salaires
COMPTA V16.05	Progiciel	Sage Edition Pilote	**2010**	Compta général/tiers
IMMO V19	Progiciel	Sage Edition Pilote	**2010**	Gestion des immos.
GEST° STOCK	Spécifique	Interne (VISUAL FOXPRO)	**1986/2001**	Suivi des stocks
GEST° INTRANT	Spécifique	Interne (VISUAL FOXPRO)	**1996**	Gestion stock intrant.

Source: Nous-mêmes, à partir du schéma directeur informatique, COTONTCHAD (1992).

Ces applications sont toutes opérationnelles. Cependant leurs interfaces sont manuelles dans la plupart des cas. Par exemple, l'inexistence de l'interface PAYE- COMPTA. La maintenance de ces applications est assurée par le personnel du département informatique actuel.

5.4.1.3. Schéma général des applications informatiques

Les schémas figurant à l'Annexe 4, page 105, présentent l'architecture générale du système d'information établie par domaine.

Le découpage en domaines (ou processus) permet de représenter le système d'information de la société selon la logique de son activité, sans tenir compte uniquement de son organisation hiérarchique et structurelle. Il est alors possible de mettre en évidence les flux d'informations entre activités de l'entreprise et les interfaces entre applications.

Ainsi, sur la base des activités de la COTONTCHAD et de l'existant des ressources informatiques, trois domaines distincts sont actuellement couverts par les applications.

- administratif;
- production;
- technique;

dans lesquels ont été précisés les sous-systèmes constitués par les applications informatiques en fonctionnement. Les domaines, tout aussi importants, comme le pilotage stratégique et le commercial ne sont pas actuellement couverts par les applications existantes. Il en est de même de nombreux autres sous-domaines tels que gestion du personnel, formation du personnel, suivi médico-social, gestion des approvisionnements, etc. également non couverts par les applications actuelles. Cependant des évolutions sont en cours pour étendre la couverture à ces domaines ou fonctions. Mais il y a lieu de doter celles qui fonctionnent actuellement d'interfaces automatiques pour pallier les contrôles manuels.

5.4.1.4. Les locaux du département informatique

Les locaux actuels du Département Informatique sont constitués de quelques cinq salles dont deux sont dédiées aux machines (salle machine) et trois bureaux.
L'une des salles machine n'est pas suffisamment vaste pour les matériels qu'elle héberge. Le système de climatisation installée est cependant très satisfaisant. Ces locaux sont implantés dans un grand bâtiment qui abrite également la Direction Financière et Comptable (DFC) et la Direction du Contrôle de Gestion et de l'Audit (DCGA).

Les locaux du département, tels que constatés présentent certaines insuffisance en matière de sécurité, notamment:

- protection incendie;
- réseaux électrique de secours;
- contrôle des accès aux salles machines
- salle d'archivage, de stockage des bandes.

5.4.1.5. Relation avec les utilisateurs

Tous les services, sans exception, sont utilisateurs actuels ou potentiels d'informatique à la COTONTCHAD, pour des besoins variés. Aussi, l'utilisation de cet outil, dans certaines

conditions n'est pas optimisée et donc ne va pas sans risque. En effet, chaque jour on fait face à de nombreux dysfonctionnements ou autres pannes des ordinateurs de bureaux ou portables, des appels pressants et plaintes des utilisateurs à l'endroit du personnel du département informatique.

5.4.1.6. Les processus informatiques

La mission et les activités de la fonction informatique décrites aux sections précédentes ont conduit à identifier les processus suivants:

- organisation de la fonction (pilotage, séparation des fonctions, compétences);
- études et développement;
- exploitation;
- maintenance des applications informatiques;
- gestion de la sécurité et continuité de l'exploitation;
- assistance aux utilisateurs.

Il convient de noter que la maintenance des matériels et autres infrastructures informatiques est assurée par le service électronique et électricité industriel placé sous la responsabilité de la Direction Technique des Usines (DTU).

Conclusion

Ce chapitre nous a permis de faire, plus ou moins, un état des lieux des ressources (personnel, matériels, logiciels, etc.) liées au système d'information de la COTONTCHAD à travers des présentations et descriptions des activités de la fonction informatique. La prise de connaissance de la fonction informatique nous a permis également de mesurer l'importance de l'informatique dans l'entreprise. Nous avons enfin, dans cette démarche, identifié les principaux processus et les principales applications existantes. Nous pouvons maintenant procéder à l'évaluation des risques informatiques, objet du prochain et dernier chapitre.

CHAPITRE VI: EVALUATION DES RISQUES OPERATIONNELS INFORMATIQUES

La prise de connaissance générale et l'étude de l'existant de la fonction informatique faite au chapitre précèdent ont permis d'identifier les principaux processus informatiques et les principales applications actuellement opérationnelles. Dans ce chapitre, il sera essentiellement question de l'analyse et l'évaluation des risques inhérents à ces processus et applications mais aussi d'évaluer le contrôle interne mis en place pour couvrir ces risques. Cette démarche nous permettra de dégager, en synthèse, les forces et les faiblesses du système en vue de formuler quelques points de recommandations à envisager pour pallier les insuffisances relevées.

L'analyse et l'évaluation des risques et du contrôle interne seront menées conformément à notre méthodologie décrite dans le chapitre précédent.

Pour mener à bien les travaux sur le terrain, notre démarche a consisté en:

- la prise de connaissance générale de la structure organisationnelle de la fonction informatique et de ses composantes;
- la consultation de la documentation, notes de service et autres éléments d'information;
- des rencontres, entretiens, interviews et échanges menés avec les principaux responsables informatiques et systèmes d'information ainsi que d'autres acteurs et utilisateurs concernés par les systèmes d'information de la société;
- un guide d'entretien avec les responsables informatiques (Annexe 5, page 106).
- questionnaire de prise de connaissance (QPC) et de contrôle interne (QCI) figurant en Annexe 7 page 111);
- des observations des locaux, des comportements du personnel et activités effectuées, dans la mesure où la plupart de celles-ci et autres opérations ne sont pas formalisées;

6.1. Identification des processus et risques associés

A l'issue de nos travaux de prise de connaissance générale, les principaux processus identifiés ainsi que les risques inhérents à ceux-ci figurent sur le tableau 14, page suivante.

Tableau 14: Matrice des processus/risques associés

item	Processus/Sous-processus	Principaux Risques (Probabilité/Impact)	Exemples de bonnes pratiques
1.	**Pilotage de la fonction**		
1.1.	Organisation interne	- Perte d'efficacité de l'organisation, des dispositifs, procédures, règlements et contrôles de sécurité; - Non atteinte des objectifs; - Mauvaise productivité des services; - Réalisation des tâches inadaptées ; - Non pérennité des modes de fonctionnement	- Existence d'un organigramme à jour; - Existence de définition de fonction ou d'attribution de chaque tâche/service; - Existence des procédures formalisées, diffusées et mise à jour régulièrement; - Existence de schéma directeur informatique et/ou plan informatique. - existence ou mise en place des structures opérationnelles.
1.2.	Compétences informatique	- Unicité de compétence; - Cumul des fonctions incompatibles; - Réalisation des tâches inappropriées; - Absence de maîtrise des volumes des travaux; - Perte d'efficacité; - Insatisfaction des utilisateurs.	- Définition claire des fonctions du personnel; - Séparation des fonctions incompatibles; - Fixation des objectifs individuels; - Limitation des habilitations; Formation générale et informatique.
1.3.	Protection et fonctionnement des dispositifs informatiques	- Altération/destruction des équipements et/ou fichiers de données; - Reprise compromise des l'exploitation;	- Existence de moyens de protection des installations, matériels sensibles et supports magnétiques: protection des accès, protection

		- Perte d'information stratégique; - Absence de maîtrise du système d"information.	contre incendie et dégâts; divers - Existence des procédures de sauvegarde; - Existence protection contre virus; - Existence plan de reprise.
2.	**Etudes et développement**	- Non fiabilité du matériel; - Non-conformité du matériel; - Pertes d'exploitation.	- Existence des plans et procédures de maintenance préventive et curative du matériel; - Qualité personnel de maintenance.
3.3.	**Accès aux systèmes informatiques**	- Perte de confidentialité et/ou Perte de qualité/intégrité des informations; - Non détection de modification de fichiers/données sensibles: - Risque de fraude; Risque financier.	- Existence de liste des autorisations d'accès aux système et applications et fichiers/données; - Existence d'une procédure formalisée d'attribution, de suppression et de mise à jour des mots de passe et codes d'accès. - Séparation dans la gestion des accès.
4.	**Gestion de la sécurité**		
4.1.	Gestion des risques informatiques		
4.2.	Sécurité physique	- Reprise compromise de l'exploitation; - Perte d'information stratégique; - Indisponibilité partielle ou totale du	- Existence de procédures de gestion des accès à la salle informatique; - Existence de moyens de protection des

		dispositif informatique. - Perte d'exploitation: vol d'information confidentielle, altération des données; - Atteinte à l'intégrité du système; - Détournement d'actifs; service dégradé.	installations, matériels sensibles et supports magnétiques, - Existence d'une protection contre les virus; - procédures de sécurité formalisées.
4.3.	Sécurité logique	- Connexion logique frauduleuse ou accidentelle entraînant détournement d'actifs matériels et immatériel; - Perte d'exploitation; - Perte d'intégrité et atteinte à la confidentialité du système.	- Existence des procédures ou définition des règles d'accès aux ressources informatiques; - Logiciel de limitation d'accès aux applications et aux composants du système; - Séparation des fonctions; - Suivi des tentatives infructueuses d'accès.
4.4.	Gestion de sauvegarde	- Risque financier; - Perte d'information stratégique; - Reprise compromise des exploitations; - Incapacité à restaurer, en priorité, les données les plus critiques; - Perte de confidentialité liée à des accès de sauvegardes non contrôlées.	- Existence ou mise en place d'une procédure périodique de sauvegardes; - Salle de confinement des sauvegardes avec des accès sécurisés et limités; - Existence ou mise en place de procédures formalisées de restauration des données.
5.	**Relations avec les utilisateurs**	- Insatisfaction des utilisateurs.	

6.2. Evaluation et hiérarchisation des risques

Tableau 15: Matrice d'évaluation des risques résiduels

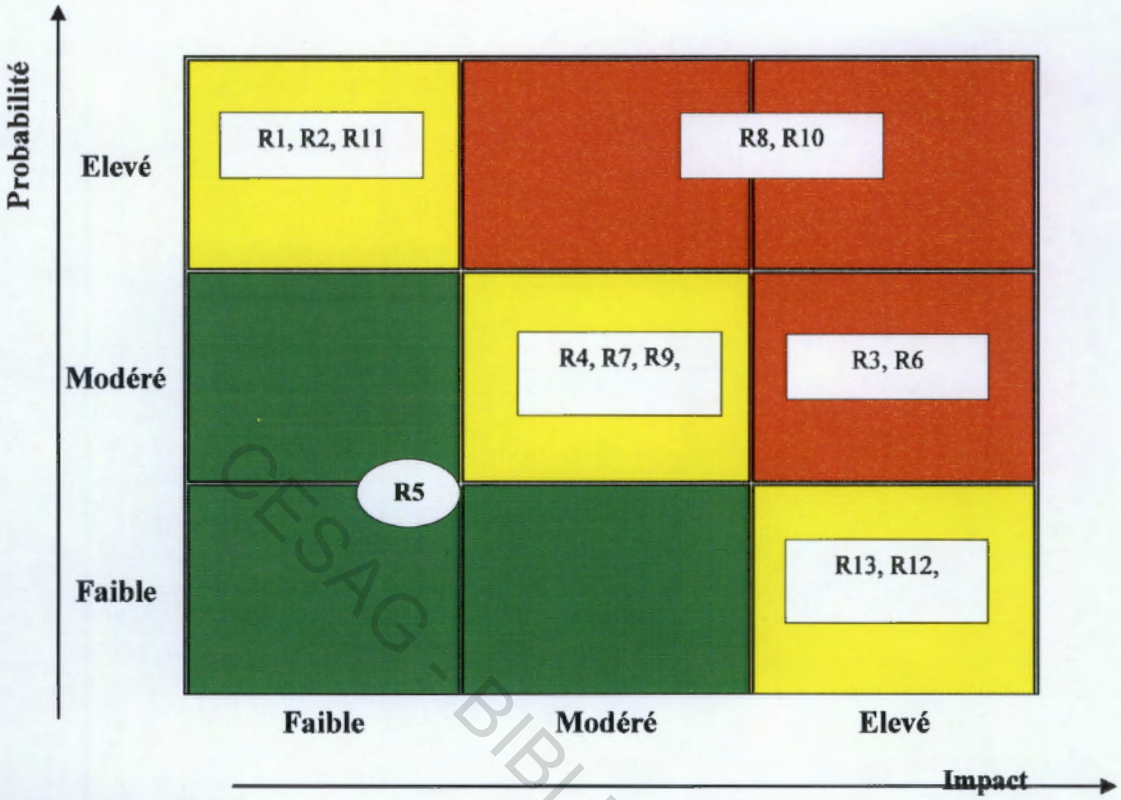
item	Processus/Sous-Processus	Risque (Rn) réel/potentiel				DMR existant		Risque résiduel	
		Risque	Pro.	Imp.	Cote	Oui/Non	Cote	Evaluation	Cote
R3	Séparation des fonctions	Fraude	3	2	2	Non	1	Elevé	3
R6	Exploitations	Travaux d'exploitation inappropriés	3	2	2	Non	2	Elevé	3
R8	Gestion des risques informatiques	Sécurité non maîtrisée	3	3	2	Non	1	Elevé	3
R10	Sécurité logique	Indisponibilité des systèmes	3	2	1	Non	1	Elevé	3
R1	Organisation de la fonction informatique	Perte d'efficacité	3	2	2	Non	1	Modéré	2
R2	Compétences informatiques	Dépendance à une personne clé	3	2	2	Oui	2	Modéré	2
R4	Etudes développement	Insatisfaction des utilisateurs	2	1		Non	1	Modéré	2

(Suite et fin tableau 15)

item	Processus/Sous-Processus	Risque (Rn) réel/potentiel				DMR existant		Risque résiduel	
		Risque	Pro.	Imp.	Cote	Oui/Non	Cote	Evaluation	Cote
R7	Maintenance informatique	Non fiabilité du matériel	2	2	**2**	Oui	**2**	Modéré	**2**
R9	Sécurité physique	Destruction / altération de l'outil informatique	2	2	**3**	Oui	**2**	Modéré	**2**
R11	Relation avec les utilisateurs	Insatisfaction des utilisateurs	3	2	**2**	Oui	**2**	Modéré	**2**
R12	Plan de reprise d'activité	Impossibilité de reprise d'activité	1	2	**1**	Non	**1**	Modéré	**2**
R13	Qualité interfaces des applications	Erreurs	3	1	**2**	Oui	**2**	Modéré	**2**
R5	Mise en service des applications	Pertes d'exploitations directes ou indirectes	2	2	**2**	Oui	**2**	Faible	**1**

Source: Nous-mêmes

Figure 5: Cartographie des risques informatiques



Source: Nous-mêmes

6.3. Identification et évaluation des risques liés à l'organisation informatique

L'organisation de la fonction informatique doit permettre de garantir un niveau de contrôle interne satisfaisant, notamment en termes de séparation des fonctions, gestion des compétences (gestion des arrivées et départs), gestion des projets et que l'ensemble des processus informatiques du département sont correctement appréhendés (pilotage, études et développement, maintenance, exploitation, sécurité du système d'information). Ce point sera abordé sous deux aspects suivants:

- organisation de la fonction informatique (séparation des fonctions);
- compétences informatiques.

6.3.1. Organisation informatique

L'analyse des facteurs de risques liés à l'organisation informatique nous a permis de situer que les différents facteurs sont totalement indépendants tout en se révélant d'un même niveau d'importance pour la société. En d'autres termes, si l'un des risques présente un niveau élevé alors le risque lié à l'organisation informatique peut être considéré comme élevé. Cette démarche de mise en œuvre des travaux ont conduit aux résultats suivants:

- absence d'organisation interne du Département Informatique;
- absence d'organigramme, définissant les relations hiérarchiques et fonctionnelles;
- absence de description des postes, des fonetions et des responsabilités de certains membres du département;
- non séparation des fonctions dans tous les domaines exercés, à savoir études et développement, exploitation, maintenances des applications, sécurités des systèmes d'information;
- absence de plan informatique;
- absence d'un schéma directeur informatique (SDI) ou plan stratégique;
- d'une façon générale, absence de formalisation des procédures et méthodes de travail;
- absence de planification, de tableau de bord et d'indicateurs de suivi des activités;
- absence de cartographie des risques informatiques;
- absence de revue de la fonction informatique par l'audit interne.

Les risques encourus sont:

- inadéquation de la stratégie informatique avec celle de la société;
- absence de planification à moyen et long terme du système d'information;
- inadaptation des ressources informatiques aux besoins de la société ou des utilisateurs;
- l'absence d'organigramme et de définition des tâches peut impliquer un excès de travail pour les uns et une incapacité à maîtriser les tâches confiées pour les autres;
- non suivi ou insuffisance des suivis des activités et performances du département;
- la non-séparation des fonctions implique un risque de fraude, malveillance, etc.;
- absence de vision globale des risques pesant sur la société en l'absence de cartographie;
- incertitudes sur les objectifs de sécurité et de contrôle de la société;

Conclusion: l'organisation de la fonction informatique présente un niveau de risque élevé.

6.3.2. Compétences informatiques

Il a été question d'examiner la qualité des compétences et d'étudier la charge de travail par rapport aux ressources humaines disponibles. Les résultats obtenus sont les suivants:

- insuffisance des compétences en rapport avec les besoins actuels et futurs, notamment dans la perspective d'un changement technologique programmée;
- insuffisance de formation continue des agents;
- excès de charge de travail: les agents touchent à tout, sans maîtrise;
- faible motivation des collaborateurs.

Les risques encourus sont:

- travail non exécuté ou mal effectué;
- continuité de l'exploitation affectée;
- dépendance à une personne clé;
- non atteinte des objectifs du département et de la société et/ou non satisfaction des besoins des utilisateurs et de l'entreprise.

Conclusion: les compétences informatiques présentent un niveau de risque élevé.

6.4. Risques liés aux études et développement

L'entretien avec les responsables les questionnaires ont conduit aux résultats suivants:

- absence de méthodologie de développement et gestion des projets déficiente;
- analyse insuffisante dans la phase des études et conception;
- objectif et périmètre du projet mal définis;
- inadéquation des méthodes, des techniques et des outils utilisés;
- absence des tests utilisateurs des applications développées;
- formation insuffisante des utilisateurs;
- documentation inexistante ou insuffisante des solutions développées;
- absence de tableaux de bord, d'outils de suivi et d'évolution des développements.

Risques réels ou potentiels:

- inefficacité globale du potentiel de développement (coût élevé, délai non respecté, ...);
- faible adéquation des solutions développées aux besoins des utilisateurs;
- insatisfaction des utilisateurs;
- perte d'efficacité et de temps;
- perte éventuelle des données;

- difficultés de maintenance et d'évolution des applications développées;
- non optimisation des ressources.

Conclusion: le processus étude et développement présente un risque modéré.

6.5. Risques liés à la mise en service des applications informatiques

Les points suivants ont été relevés:

- absence de séparation des tâches entre études et exploitation;
- documentation technique inexistante ou insuffisante;
- tests exécutés sans le recours d'une méthodologie appropriée;
- absence d'interfaces automatiques entre les applications "Paie", "Gestion de production – Evacuation", "Gestion des stocks", "Gestion des intrants " et comptabilité générale et tiers".
- absence de plan de reprise des données;

Risques réels ou potentiels:

- pertes d'exploitation directes ou indirectes relativement importantes;
- perte d'efficacité du dispositif et erreurs pouvant entrainer tout type de sinistre;
- absence de maîtrise du système d'information;
- reprise compromise de l'exploitation.

Conclusion: le risque lié à la mise en service des applications informatiques est élevé.

6.6. Risques liés au processus exploitation

Les principales faiblesses relevées au niveau du processus exploitation peuvent être résumés comme suit :

- absence de procédures formalisées de gestion de l'exploitation informatique;
- absence de tableaux de bord et d'outils de suivi de l'exploitation;
- absence de registre de suivi des incidents informatiques et des problèmes des utilisateurs;
- absence d'outil de suivi de performance du réseau.

Risques encourus:

- travaux d'exploitation non réalisés de façon appropriée;
- suivi non satisfaisant des incidents informatiques et des problèmes des utilisateurs;
- restauration incorrecte des fichiers après incidents;

- programmes exécutés avec les mauvaises données;
- répétition d'erreurs de traitement;
- difficultés à identifier les problèmes du réseau et à suivre sa performance.

Conclusion: le processus exploitation présente des risques de niveau élevé.

6.7. Risques liés au processus maintenance informatique

Il s'agit aussi bien de la maintenance des matériels que de celle relative aux applications.

6.7.1. Maintenance des applications informatiques

Toute application, quelque soit son degré de perfection, nécessite, à un moment ou à un autre, la correction de problèmes ou l'adjonction de fonctions supplémentaires. La maintenance et l'évolution des applications développées est d'importance capitale dans la mesure où, très souvent, le système d'information d'une entreprise repose seulement sur quelques applications stratégiques.

L'étude de l'existant révélé les risques réels ou potentiels suivants:

- pertes d'exploitation si l'application ne donne pas les résultats attendus, d'où dysfonctionnement, erreurs et perte de temps;
- modifications entrainant la destruction des verrous de sécurité préexistants;
- maintenance rendue impossible suite à indisponibilité des personnes compétentes;
- préjudice pour la société en cas de modifications frauduleuses si les opérations de maintenance ne sont pas bien respectées ou mal effectuées.
- incapacité à faire évoluer les applications, en adéquation avec les besoins de la société;

Conclusion: le processus maintenance des applications présente un risque modéré.

6.7.2. Maintenance des matériels informatiques

La fonction informatique ne peut garantir un service de qualité que dans la mesure où son parc de matériels (y compris tous les constituants) fonctionne sans incident majeur. Ce qui implique que le choix de matériel et du constructeur ou du fournisseur sont des facteurs importants à prendre en compte. Les risques de maintenance de matériels identifiés peuvent être résumés comme suit:

- pertes ou retard d'exploitation ou dysfonctionnement du matériel suite à des livraisons non conformes;
- indisponibilité du matériel du fait qu'il est mal maîtrisé par le fournisseur:
- manque de fiabilité du matériel, en ce sens que si le matériel tombe souvent en panne et que son utilisation est sur le chemin critique de la production, les retards accumulés peuvent engendrer des pertes opérationnelles ou financières conséquentes. Il en est de même si les données lues par le matériel ne sont pas restituées correctement; les erreurs ainsi générées sont source de sinistres immatériels.

Il convient de noter que la maintenance des matériels informatiques n'est pas du ressort du département informatique mais relève du service d'électricité industriel, structure rattachée à la Direction Technique des Usines. Nous avons relevé au niveau de cette entité des procédures formalisées de maintenance préventive et curative des matériels. Cependant les délais d'intervention, de réponse des réparations sont très longs. Le suivi des réparations des pannes et incidents de matériels sont insuffisants ou parfois défaillants.
Conclusion: le processus maintenance des matériels informatiques présente un risque modéré.

6.8. Risques liés aux relations avec les utilisateurs et assistance

Les systèmes informatiques sont utilisés pour automatiser certaines transactions de l'entité et pour satisfaire ses besoins. Il est donc important de savoir si les utilisateurs sont satisfaits par ces systèmes et par les services offerts par le département informatique. Les interviews et entretiens menés avec les utilisateurs du système d'information ont porté essentiellement sur les aspects suivants:

- fiabilité et exhaustivité des données restituées par le système d'information;
- qualité de couverture fonctionnelle des applications par rapport aux besoins des utilisateurs;
- stabilité du système en termes de performance, de fonctionnalité, de résultat, et de reporting, etc., nécessitant peu de maintenance de la part du département informatique;
- qualité et rapidité des services rendus et assistance aux utilisateurs;
- formation des utilisateurs par rapport à l'utilisation des ressources informatiques mises à leur disposition.

Les points suivants ont été relevés:

- formation insuffisantes des utilisateurs à l'utilisation des ressources informatiques;
- absence d'un service support aux utilisateurs (helpdesk);
- absence de charte des utilisateurs du système d'information;
- insuffisance de couverture fonctionnelle des applications informatiques et interfaces;

Risques réels ou potentiels:

- utilisation inadéquate des ressources informatiques et non respect du principe de confidentialité par les utilisateurs;
- mauvaise manipulation des applications par les utilisateurs;
- fiabilité et exhaustivité non garantie des données restituées.
- incapacité du département à répondre rapidement aux demandes des utilisateurs;
- inefficacité ou manque de ressources du département pour intervenir rapidement ou encore inadaptation des ressources aux services requis par les utilisateurs.
- insatisfaction des utilisateurs par rapport aux applications mises à leur disposition;
- incapacité du département informatique à hiérarchiser les demandes de modification des programmes émises par les utilisateurs.

Conclusion: le processus relations utilisateurs et assistance présente un risque modéré.

6.9. Risques liés à la gestion de la sécurité et continuité d'exploitation

L'étude de l'existant a porté essentiellement sur les points suivants:

- gestion des risques informatiques;
- sécurité physique
- sécurité logique;
- plan de continuité ou plan de reprise d'activité/plan de secours.

6.9.1. Risques liés au processus gestion des risques informatiques

Les points suivants ont été relevés:

- absence de procédures d'analyse et d'évaluation des risques informatiques;
- absence de cartographie des risques informatiques;
- absence de sensibilisation des utilisateurs et autres acteurs aux risques informatiques.
- absence de plan et mesures de sécurité relatives aux infrastructures et applications;
- absence de mise à jour ou mise à jour irrégulière d'anti virus sur les serveurs et les postes de travail des utilisateurs;

Risques réels ou potentiels:

- méconnaissance des risques auxquels est exposée la fonction informatiques;
- vulnérabilité élevée des infrastructures et applications informatiques;
- sécurité non maîtrisée;
- fiabilité et exhaustivité non garantie des données restituées.

Conclusion: le processus évaluation et gestion des risques présente un risque élevé.

6.9.2. Risques liés à la sécurité physique

Par entretiens avec le responsable informatique et les collaborateurs, les points suivants ont été abordés de façon globale:

- infrastructures, réseau, salle serveurs;
- sécurité des traitements informatiques;
- intégrité des informations détenues dans l'entreprise;
- disponibilité du système informatique;
- procédures de gestion des sauvegardes, de restauration des données sauvegardées et de surveillance, dispositifs propres à assurer la continuité d'exploitation;
- intrusion externe et internet.

A l'issue des entretiens, les points suivants ont été relevés:

- absence de politique de sécurité bien définie et connue de tous;
- insuffisance/absence des moyens ou systèmes adéquats de protection des ressources informatiques contre les pirates, les virus, les pannes électriques, la fraude, etc. ;
- absence ou insuffisance des contrôles des accès physiques aux locaux et ressources;
- absence de règlementation des mesures de sécurité physique et de protection des ressources informatiques sensibles et d'accès aux locaux hébergeant ces ressources;

Les risques suivants, réels ou potentiels ont été relevés:

- destruction/altération de l'outil informatique et/ou fichiers des données;
- infection des micros ordinateurs, des fichiers ou données par les virus;
- vol d'informations confidentielles, altération et atteinte à l'intégrité des données
- altération du matériel ou des fichiers par un tiers, perte d'informations stratégiques;
- accès non autorisé des tiers aux ressources informatiques, vol, malveillance;
- absence de maîtrise des systèmes d'information;
- coupures de courant entraînant des surtensions, pannes, incendie;

- d'une façon générale, indisponibilité du système d'information et donc continuité d'exploitation compromise.

Conclusion: la sécurité physique présente un risque élevé.

6.9.3. Risques liés à la sécurité logique

La sécurité logique correspond aux risques d'accès aux données par des personnes non autorisées (internes ou externes), ainsi qu'aux risques d'altération des données par des virus. Pour ce faire, il importe de mettre en place un dispositif adapté à la prévention de ces risques. Les aspects suivants ont été abordés lors de notre entretien avec les acteurs concernés:

- politique de sécurité logique;
- gestion des mots de passe et des habilitations (surveillance de l'accès aux données sensibles, utilisation d'internet/messagerie, mise à jour d'antivirus, protection contre les attaques externes, etc.);
- sensibilisation du personnel à la sécurité logique;
- procédures de création, modification, suppression, et de revue utilisateurs;
- séparation des fonctions.

Nous avons relevé les insuffisances suivantes:

- absence de politique formalisée de sécurité logique et procédures de gestion des habilitations dans les systèmes d'information;
- absence de séparation de fonction;
- absence de mise à jour des listes des personnes autorisées à accéder aux systèmes informatiques;
- absence de procédures formalisées de mise à jour d'antivirus sur les postes de travail;
- absence de règlementation d'accès à l'internet, messagerie et utilisation des clés USB;
- d'une façon générale, accès au système d'information non contrôlé.

Risques réels ou potentiels:

- l'accès non autorisé peut occasionner soit des modifications non autorisées des programmes soit des modifications et suppressions des données ou fichiers;
- perte de confidentialité, de qualité et/ou d'intégrité des informations;
- absence de détection de modification de fichiers des données sensibles, fraude et malveillance;

- perte d'exploitation due au non fonctionnement des logiciels de base et des applications ou encore à une mauvaise organisation des accès aux applications;
- destruction des données suite aux infections des virus informatiques;
- d'une façon générale, indisponibilité des systèmes.

Conclusion: la sécurité logique présente un risque élevé.

6.9.4. Risques liés à la continuité de l'activité

Cette section traite des différents problèmes liés au plan de reprise en cas d'incident en considération de la continuité des opérations classiques d'informatiques. L'impact d'une perte de traitements informatiques peut varier de façon significative selon les applications d'une même entité au sein de la société, (par exemple: incident dans l'application paie à la fin du mois). Aussi, deux aspects seront considérés dans la perspective de continuité de l'activité à savoir les sauvegardes et le plan de reprise en cas d'incident.

- *Sauvegardes*

  Les points suivants ont été relevés:
- les sauvegardes des données et des programmes, applications et logiciels de base sont effectuées quotidiennement et régulièrement.
- les sauvegardes effectuées ne sont pas stockées en lieux sûrs ou hors site d'exploitation. Les sauvegardes sont conservées au niveau du département informatique mais elles ne sont pas stockées dans un local ignifuge;
- absence des tests de reprise des sauvegardes pour s'assurer que les données et les programmes peuvent être utilisés rapidement, facilement et sont lisibles;
- absence de tests sur le temps nécessaire pour redémarrer le système, essentiel pour assurer le succès de sauvegardes et de reprise de l'activité;
- des données importantes pour l'entité se trouvant souvent dans les micro-ordinateurs, un contrôle trop faible sur ceux-ci, particulièrement en ce qui concerne les sauvegardes, risque de faire perdre à l'entité accidentellement ou intentionnellement ses données sensibles stockées sur les micro-ordinateurs.

Conclusion: le processus sauvegardes présente un niveau de risque modéré.

- *plan de secours ou plan de reprise en cas d'incident*

Un incident est une action capable d'entraver la bonne marche des opérations, allant de la petite interruption à la catastrophe. Un incident sur une application essentielle de l'entité peut mettre en péril toute la pérennité de l'entité ; des incidents mineurs peuvent aboutir à des dépenses inutiles et des blocages systèmes inacceptables pénalisant l'exploitation.

Les points suivants relatifs au plan de reprise de l'activité ont été relevés:

- absence de plan de reprise défini, documenté et distribué aux personnes responsables de sa mise en œuvre;
- absence de tests de reprise d'activité en cas d'incident ou de sinistre particulier.

Risque réel ou potentiel:

- impossibilité de reprendre correctement son activité (en termes de délai et d'efficacité) en cas d'incident;
- un incident sur une application critique peut toucher l'ensemble de l'activité de l'entité voire sa pérennité, ce risque variant selon les applications.

Conclusion: l'absence de plan de reprise de l'activité génère un risque élevé.

6.10. Identification et évaluation des risques et des contrôles d'application

Cette étape nous permettra de recenser et d'évaluer les risques impactant les processus applicatifs identifiés. De même, nous procéderons à l'identification des contrôles applicatifs destinés à couvrir les risques pesant sur le bon fonctionnement des applications afin d'isoler ceux n'ayant pas été couverts par les contrôles en place et qui constituent encore des facteurs de vulnérabilité des systèmes applicatifs. Des recommandations ou des mesures des bonnes pratiques en matière de contrôle interne peuvent alors être proposées pour les contenir.

6.10.1. Risques lies aux applications

L'identification des risques liés aux applications nous a conduits à retenir les risques inhérents tels que:

- la possibilité de saisie des données erronées ou non autorisées;
- la possibilité de modifier, supprimer ou d'ajouter des données sans autorisation;
- l'absence de procédure d'identification, de correction et de recyclage des données rejetées;
- le traitement erroné ou incomplet des données;

- l'exécution de traitement non autorisée;
- l'absence de contrôle d'intégrité des données saisies, traitées et éditée;
- l'absence de contrôle du contenu et de la destination des résultats des états de sortie;
- l'absence de contrôle sur le traitement et la transmission des fichiers.

6.10.2. Les contrôles d'applications

Les contrôles d'application sont conçus et mis en place afin d'assurer l'intégrité des enregistrements, ils peuvent être manuels ou automatiques, préventifs, détectifs ou correctifs. Ils donnent une assurance directe quant à la fiabilité des enregistrements.

Les contrôles préventifs ont pour objectif de prévenir la survenance d'anomalies d'erreurs ou de fraude aussi bien au niveau des entrées et des traitements qu'au niveau des sorties. En revanche, les contrôles détectifs permettent l'identification de ce type d'évènement.

Les contrôles correctifs visent à minimiser l'impact des erreurs ou anomalies et fraudes découvertes. Ils permettent non seulement de les corriger et de les recycler mais aussi de modifier les processus du système de façon à éviter qu'elles se reproduisent dans l'avenir.
Nous allons considérer ces contrôles en relation avec les principales étapes des processus d'une application à savoir:

- entrées;
- traitements;
- sorties;
- recyclage des rejets et des erreurs.

6.10.3. Les contrôles des Entrées

Les procédures de contrôle sont mises en œuvre afin de garantir l'autorisation, l'exactitude, l'existence, et l'exhaustivité des transactions et des données permanentes.
Nous avons mené des entretiens avec les responsables, notamment sur les points concernant:

- les procédures de contrôle d'accès;
- les procédures de la collecte et la saisie des transactions et des données;
- les procédures de traitement des données rejetées.

6.10.4. Contrôle d'accès aux applications

Ces contrôles prévus et mis en œuvre dans le système doivent permettre de restreindre l'accès aux données, aux programmes et aux transactions aux seules personnes qui y sont habilitées. Parmi ces contrôles nous pouvons citer:

- une gestion appropriée des mots de passe définie en fonction des ressources à partager (unicité de l'identifiant, absence de compte générique, longueur des mots de passe et leur changement périodique).
- des procédures de détection et de contrôle des tentatives infructueuses des accès non autorisés;
- le respect du principe de séparation des tâches;
- des procédures de partage de l'accès aux données et aux transactions en fonction des profils et des tâches des utilisateurs et des informaticiens.

Les insuffisances suivantes relatives à l'accès aux applications ont été relevées:

- absence de procédures formalisées d'accès aux ressources logiques;
- absence de mis à jour des mots de passe et de changement périodique;
- existence des profils ou comptes génériques des utilisateurs au sein des applications.

Risque réel ou potentiel:

- accès non autorisé par des tiers internes ou externes aux données sensibles;
- impossibilité de retracer les opérations faites par les utilisateurs;
- altération, destruction ou modification des programmes, données et fichiers;
- atteinte à l'intégrité et à la confidentialité des données sensibles;
- non protection des informations sensibles;
- absence de séparation des tâches (entre informaticiens, utilisateurs, informaticiens et utilisateurs).

Conclusion: le contrôle d'accès aux applications présente un risque élevé.

6.10.5. Contrôle de la collecte et la saisie des données

Les procédures devraient permettre de garantir que toutes les transactions et les données nécessaires sont collectées de façon exhaustive et qu'elles sont enregistrées d'une manière exacte et exhaustive. Nous avons relevé que ces procédures existent mais ne sont pas formalisées et mises à la disposition des utilisateurs.

6.10.6. Contrôle de l'enregistrement des données

Les contrôles automatiques et manuels concernent essentiellement l'enregistrement des données en considérant les aspects de contrôle suivant: autorisation, exactitude, et exhaustivité des données saisies et validité, identification et correction des erreurs et anomalies…etc. Nous nous sommes intéressés aux points de contrôle relatifs à:

- l'autorisation de toutes les données et les transactions enregistrées dans le système;
- l'interdiction de la saisie des données non valides (Exemple: mise en place de format des données permettant de limiter la saisie des données non valides à savoir des champs de saisie);
- la détection des doubles-saisies, des saisies incomplètes, et des incohérences;
- la réconciliation des brouillards de saisie avec les documents sources;
- la saisie des données permanentes;
- la garantie de l'unicité de la saisie des données ;
- les rapprochements automatiques des données avec celles déjà saisies;
- la vérification de la séquence numérique;
- la réconciliation des totaux des données saisies (réconciliation manuelle ou automatique);
- la mise à jour des fichiers;
- la vérification de l'exhaustivité et exactitude des fichiers ou entrées (tout fichier transmis doit contenir des zones de contrôle de l'exhaustivité et l'exactitude des données transmises (contrôle des doublons, des trous, de la longueur et nombre des transactions).

Il y a lieu de noter qu'il existe plusieurs types de contrôle des enregistrements que les entreprises peuvent mettre en place au niveau des applications informatiques. Parmi ces contrôles, nous pourrons citer à titre d'exemple:

- les contrôles batch: Ils permettent le contrôle des totaux et ils peuvent porter sur un total monétaire, le nombre d'articles ou le total des documents saisis;
- les contrôles de la séquence: Ils sont conçus de façon à ce que seules les données comprises dans la séquence prévue soient admises et que les doublons soient rejetés;
- les contrôles de limite: Ils sont conçus de façon à ce que seules les transactions n'excédant pas une certaine limite puissent être traitées;

- les contrôles selon certains paramètres: Les données sont acceptées par le système selon des critères prédéterminés;
- les contrôles de double-saisie: La nouvelle transaction est comparée avec celle ou celles déjà saisie(s). Si une redondance est détectée, elle sera rejetée;
- les contrôles de vraisemblance: La vraisemblance des données est contrôlée selon une logique prédéterminée.

Aussi, il serait judicieux de prévoir des procédures permettant la conservation, la vérification, l'analyse et le recyclage des données rejetées par le système. A cet effet; nous avons relevé les observations suivantes:

- certains de ces contrôles ci-haut énumérés existent mais ne sont pas entièrement appliquées. Les autres contrôles, par contre, n'existent pas du tout.

Risques réels ou potentiels:

- non exhaustivité et exactitude des données enregistrées;
- erreurs de saisie et anomalies relatives aux opérations d'enregistrement des données.

Conclusion: le processus contrôle des enregistrements des données présente un risque modéré.

6.10.7. Contrôle des traitements et des sorties des données

Ces contrôles ont pour objectif d'assurer l'exhaustivité l'exactitude et la réalité des données accumulées. Les points suivants ont fait l'objet d'entretien avec les responsables:

- toutes les opérations traitées sont-elles journalisées?
- les totaux de fin de traitement font-ils l'objet des contrôles et des comparaisons?
- l'intégrité des données est-elle assurée?
- les états de sorties sont-ils testés et contrôlés avant leur distribution?
- les résultats des sorties sont-ils validés par les utilisateurs?

Il faut noter qu'il existe plusieurs types de contrôles des traitements que les entreprises peuvent mettre en place au niveau des applications. Parmi ces contrôles de traitement, nous pouvons citer à titre d'exemples:

- le calcul manuel: Sélectionner un échantillon des transactions et recalculer manuellement puis comparer le résultat avec le traitement du système;
- le contrôle de limite;
- le contrôle de vraisemblance;

- les rapports d'exception ou d'anomalies: Un rapport d'exception qui génère les données erronées compte tenu de certains critères prédéfinis.

Les observations suivantes ont été relevées:

- absence de certains contrôles sur des données issues des traitements:
- insuffisance des contrôles des anomalies relevées;
- absence de recyclage des données rejetées;
- certaines fonctionnalités temporaires des applications ne se désactivent pas automatiquement après clôture des opérations de la période.

Risques réels ou potentiels:

- répétition des erreurs ou anomalies commises auparavant;
- non exhaustivité et exactitude des résultats obtenus des traitements des données.

Conclusion: le processus traitement et sortie des données présente un risque modéré.

6.10.8. Les contrôles sur les interfaces d'application

Les applications présentes et la manière dont elles sont interfacées doivent être adaptées à la structure mise en place (volumétrie, type d'activités gérées ...), mais doivent garantir la disponibilité et l'intégrité des données de la saisie initiale à la production des états.
L'analyse des interfaces reliant les applications a concerné essentiellement les aspects suivants:

- qualité des interfaces;
- niveau de stabilisation des interfaces;
- modalité de retraitement des anomalies identifiées lors des interfaces avec la comptabilité.

6.10.9. Qualité des interfaces entre application de gestion et comptabilité

Les observations suivantes ont été relevées:

- la plupart des interfaces sont manuels (saisies, validation manuelle nécessaire), seule l'application "Gestion des immobilisations" présent l'interface automatique avec la comptabilité
- l'interface automatique génère parfois des anomalies éditées sur des états sous forme de "compte rendu d'anomalie", permettant de comparer les données en entrées et en

sorties du traitement de l'interface mais personne n'est désigné ou ne se sent responsable de ces anomalies.

- les états d'anomalie ne sont parfois pas correctement analysés, donnant lieu à des corrections incomplètes et inappropriées. Les états d'anomalies sont supprimés sans avoir été analysés et traités. Les informations ou écritures sont peut être définitivement perdues ou doivent être reconstituées manuellement (lorsque cela est possible).

Risques réels ou potentiels:

- erreurs de saisie, manipulations oubliées, doubles saisies, etc.

Conclusion: en l'absence d'interface automatique, le niveau de risque est élevé.

6.10.10. Niveau de stabilisation de l'interface

L'interface "Gestion des immobilisation/comptabilité" étant récente, elle présente une certaine fiabilité malgré des problèmes rencontrés au début de son installation et paramétrage.

6.10.11. Mode de traitement des anomalies

Les anomalies constatées ne sont pas traitées, ni de manière appropriée ni périodiquement ni suivant un mode de retraitement connu (recyclage, suppression). Le département informatique a la responsabilité de la correction des anomalies constatées lors des interfaces. Mais il arrive parfois que ces anomalies ne soient jamais retraitées.

Risques réels ou potentiels:

- non satisfaction des utilisateurs, propriétaires des données traitées;
- absences de solutions durables quant aux anomalies constatées.

Conclusion: le mode de traitement des anomalies présente un niveau de risque modéré.

6.11. Synthèse des points forts et des faiblesses identifiés

L'étude que nous avons menée dans l'optique d'évaluation des risques nous a permis de couvrir une préoccupation majeure à savoir le niveau des risques induit par la possession et l'utilisation de l'outil informatique et, dans une certaine mesure, le potentiel d'optimisation. Il y a donc lieu de dégager les points forts et les points faibles mais aussi et surtout des recommandations à mettre en œuvre afin d'améliorer le fonctionnement du système. Ces recommandations concernent particulièrement la fonction informatique, les applications et

infrastructures et les relations avec les utilisateurs. La synthèse des points forts et des points faibles constatés figure en Annexe 6, page 107.

6.12. Recommandations spécifiques ou bonnes pratiques de contrôles internes

Les recommandations que nous proposons concernent essentiellement les aspects généraux des systèmes d'information à savoir, l'organisation de la fonction et l'environnement informatiques sans lesquels les applications ne fonctionneraient pas. Ce qui sous entend que nos recommandations proposées seront axées sur la fonction et l'environnement informatiques et de ce fait emporteraient les recommandations sur les applications.

Les recommandations les plus importantes, eu égard à l'ampleur du sujet traité, concernent essentiellement les aspects suivant:

- l'organisation de la fonction informatique;
- les principaux processus informatiques;
- l'accès aux systèmes informatiques;
- la sécurité de l'environnement informatique (sécurité physique, sécurité logique et gestion des sauvegardes, plan de continuité d'activité ou plan de reprise);
- la gestion des relations avec les utilisateurs.

Les propositions de recommandations, relatives à ces domaines, sont récapitulées sur le tableau 16 de la page suivante.

Tableau 16: Propositions de recommandations

DOMAINE / POCESSUS	RECOMMANDATIONS	OBSERVATIONS
1. Fonction informatique	1. - Mettre en place une structure d'organisation opérationnelle comprenant au moins: – Equipe Etudes et développement; – Equipe système et exploitation informatiques; – Equipe réseau, sécurité et assistance utilisateurs. 2. - Séparer les fonctions incompatibles; 3. - Mettre en place un organigramme et des description des tâches ou fonctions.	
1.1. Organisation interne de la fonction		
1.2. Compétences informatiques	1. – Recruter du personnel compétent et motivé; pour renforcer l'effectif actuellement insuffisant en nombre et compétence; 2. – Mettre en place un système de planification et de suivi des tâches des agents du département; 3. Définir un plan de formation continue du personnel informaticien.	
2. Les études et développement	1. –impliquer les utilisateurs dans les différentes phases de développement interne ou dans les processus d'acquisition des applications; 2 - Séparer l'équipe de développement de celle d'exploitation; 3 Former les utilisateurs lors des installations ou modifications des programmes et applications.	
3. Mise en service des applications et exploitation informatiques	1. - Séparer l'exploitation de l'activité étude et développement;	
4. Maintenance	1. – Rattacher le service de maintenance, actuellement sous la responsabilité de la Direction Technique de Usine, au Département Informatique; 2. – Renforcer les procédures de maintenance préventive et alléger celles relative à la maintenance curative des équipements; 3. – Personnel de qualité et compétent pour assurer la maintenance des équipements.	
4.1. Maintenance des matériels		
4.2. Maintenance des applications	1 – Formaliser des procédures à suivre en cas de dysfonctionnement des applications ou programmes 2. - Mettre en place un journal des indisponibilités des applications; programmes et autres logiciels; 3 – Mettre en place un registre de recueil des incidents	

5. Sécurité et continuité de l'exploitation *5.1 Gestion des risques informatiques*	1. - Définir des moyens permettant de reprendre l'exploitation en cas de panne ou de perte importante de données (plan de reprise, contrat de maintenance) 2. – Etablir une cartographie des risques informatiques 3. – Nommer un responsable chargé de la sécurité et de la gestion des risques informatiques.	
5.2. Sécurité physique	1. - Mettre en place des moyens de gestion des accès à la salle informatique ou de restriction des accès aux seules personnes autorisées. 2.- Déployer des moyens adéquats destinées à protéger les installations, équipements sensibles, et supports magnétiques 3. – Installer et vérifier régulièrement les moyens de protection anti virus et mettre en place d'autres moyens de sécurité (coupe feu).	
5.3. Sécurité logique	1. - Etablir la liste des autorisations d'accès au système d'information, aux applications et aux fichiers/données sensibles; 2. – Formaliser une procédure d'utilisation (arrivée, mutation), de suppression et de mise à jour des mots de passe et des codes d'accès; 3 – Revoir périodiquement la liste des login et mots de passe actifs;	
5.4. Plan de continuité: – *Sauvegardes* – *Assurance*	1. - Mettre en place une procédure périodique de sauvegarde automatisée des données; 2. - Aménager une salle de conservation des sauvegardes avec des accès sécurisés e limités 3 – Mettre en place des procédures formalisées de restauration des données et les tester périodiquement;	
6. Assistance aux utilisateurs	1. - Mettre en place un service d'assistance aux utilisateurs; 2. - Enquêtes de satisfaction auprès des utilisateurs et autres acteurs du système d'information; 3. - Former les utilisateurs aux manipulations correctes de l'outil et applications informatiques.	

Source: Nous-mêmes

La mis en œuvre de ces recommandations sera discutée avec les acteurs concernés, en particulier le responsable du département informatique de la COTONTCHAD. Celui-ci connait mieux les priorités, difficultés et contraintes de son département pour faire des choix judicieux parmi ces recommandations afin de réorganiser au mieux son entité.

Conclusion

Ce chapitre a été pour nous l'occasion de mise en œuvre concrète de notre méthodologie d'étude précédemment décrite au chapitre 3. La prise de connaissance générale de la fonction informatique, complétée des entretiens, interviews, observations et tests sur certains points de contrôle des processus informatiques et applicatifs, nous a permis d'identifier les risques se rapportant à ces processus. Nous avons identifié ces risques qui sont plus ou moins, élevés aussi bien sur les processus informatiques que sur ceux relatifs aux applications. Dès lors, nous avons dégagé les points forts et les points faibles du système d'information, ainsi que les recommandations qui s'imposent aux faiblesses constatées.

CONCLUSION DE LA DEUXIEME PARTIE

Cette deuxième partie de notre étude a permis de présenter la société cotonnière du Tchad "COTONTCHAD", avec ses objectifs et mission ainsi que les traits caractéristiques de son organisation et fonctionnement internes.

La cartographie élaborée à l'issue de l'évaluation des risques nous à permis de constater que la fonction informatique et les processus gérés sont l'objet de grandes menaces. Ces risques doivent être contenus d'une façon ou d'une autre pour sécuriser au mieux les systèmes. Le tableau des forces et faiblesses que nous avons dégagées permet de réfléchir à ce sujet.

A partir des forces et faiblesses constatées, nous avons proposé quelques points de recommandations à mettre, plus ou moins, en œuvre afin d'améliorer, si possible, le bon fonctionnement du système d'information (fonction informatique, applications, relation avec les utilisateurs).

CONCLUSION GENERALE

L'informatique et le système d'information de l'entreprise qu'elle supporte sont au cœur des activités de celle-ci par l'enregistrement, le traitement, la restitution et la conservation des informations qui, du reste, peuvent se révéler stratégiques pour la société. Cet outil, plus qu'une nécessité, est devenu incontournable pour l'entreprise dans ce monde de communication, de mondialisation mais en perpétuelle mutation. De ce fait, si la possession de l'outil informatique est une nécessité incontournable pour les organisations ouvertes au mode extérieur, il expose celles-ci, par la même occasion, à des risques qui peuvent menacer leur devenir, voire leur survie. Il devient dès lors important de connaitre ces risques afin de mettre en place des mesures pour protéger les ressources informationnelles de la société.

La connaissance des risques informatiques et ceux liés aux applications qui l'accompagnent suppose la mise en œuvre d'une méthodologie d'évaluation des risques basée sur les référentiels reconnus et cadrés des normes professionnelles mais aussi et surtout des bonnes pratiques communément admises.

Notre démarche méthodologique, décrite d'abord sous son aspect théorique au travers des revues de la littérature sur le sujet, a été ensuite déclinée en pratique qui a permis d'aborder, dans la réalité, la problématique des risques liés aux applications informatiques de la COTONTCHAD.

Cette démarche, technique et méthodologique, mise en œuvre au travers de certains outils d'analyse et de diagnostic, nous a conduits à l'étude de l'existant de l'entité en charge de la fonction informatique de la COTONTCHAD. Ceci a été fait après une brève présentation de celle-ci et de son Département Informatique (DI) que nous avons présenté da manière détaillée en mettant en évidence ses processus informatiques et applicatifs. .

L'identification et l'évaluation des risques, objet de notre étude, a été effectué à partir des processus informatiques et applicatifs identifiés. Nous avons également identifié et évalué les contrôles applicatifs en place. A l'issue de ces travaux, nous avons dégagé les points forts et les points faibles de l'entité en charge de la fonction informatique. Nous avons, à cet effet, émis quelques recommandations, plus ou moins pertinentes, afin d'améliorer le fonctionnement actuel du système d'information de la COTONTCHAD.

ANNEXES

ANNEXE 1: informations caracteristiques de la cotontchad

1.1. Caractéristiques et capacités réelles de production annuelle des usines d'égrenage de la COTONTCHAD: base campagne cotonnière de 150 jours.

	Type égreneuse	Nombre d'égreneuse	Nombre scies	Capacité jour production (T)	Capacité prod. Campagne (T)	Observation
DOBA	120 Scies	3	360	112	**16.800**	Fermée
G. GAYA	120 Scies	3	360	112	**16.800**	Fermée
KELO	141 Scies	3	423	150	**42.000**	
KOUMRA	120 Scies	5	600	180	**27.000**	
KYABE	120 Scies	2	240	60	**9.000**	Fermée
LERE	120 Scies	3	360	60	**16.800**	
MOUNDOU	141 Scies	4	360	350	**52.500**	
PALA	141 Scies	3	423	280	**42.000**	
SARH	120 Scies	5	600	180	**27.000**	
TOTAL		**31**	**3.726**			

Source: COTONTCHAD, Direction Technique des Usines (DTU).

1.2. Evolution de la production coton graine et fibre des cinq dernières années

	2007	2008	2009	2010	2011
Production c/g (t)	98 055	100 770	70 977	35 092	52 569
Production fibre (t)	40 229	40 136	28 574	14 038	21 355

Source: COTONTCHAD / Direction Technique des Usines (DTU).

1.3. Evolution de l'effectif du personnel et de la masse salariale des cinq dernières années

	2007	2008	2009	2010	2011
Effectif pers.	2 070	2 061	969	815	900
Masse sal. (en millier)	4 315 620	3 291 116	3 655 621	3 982 326	4 349 373

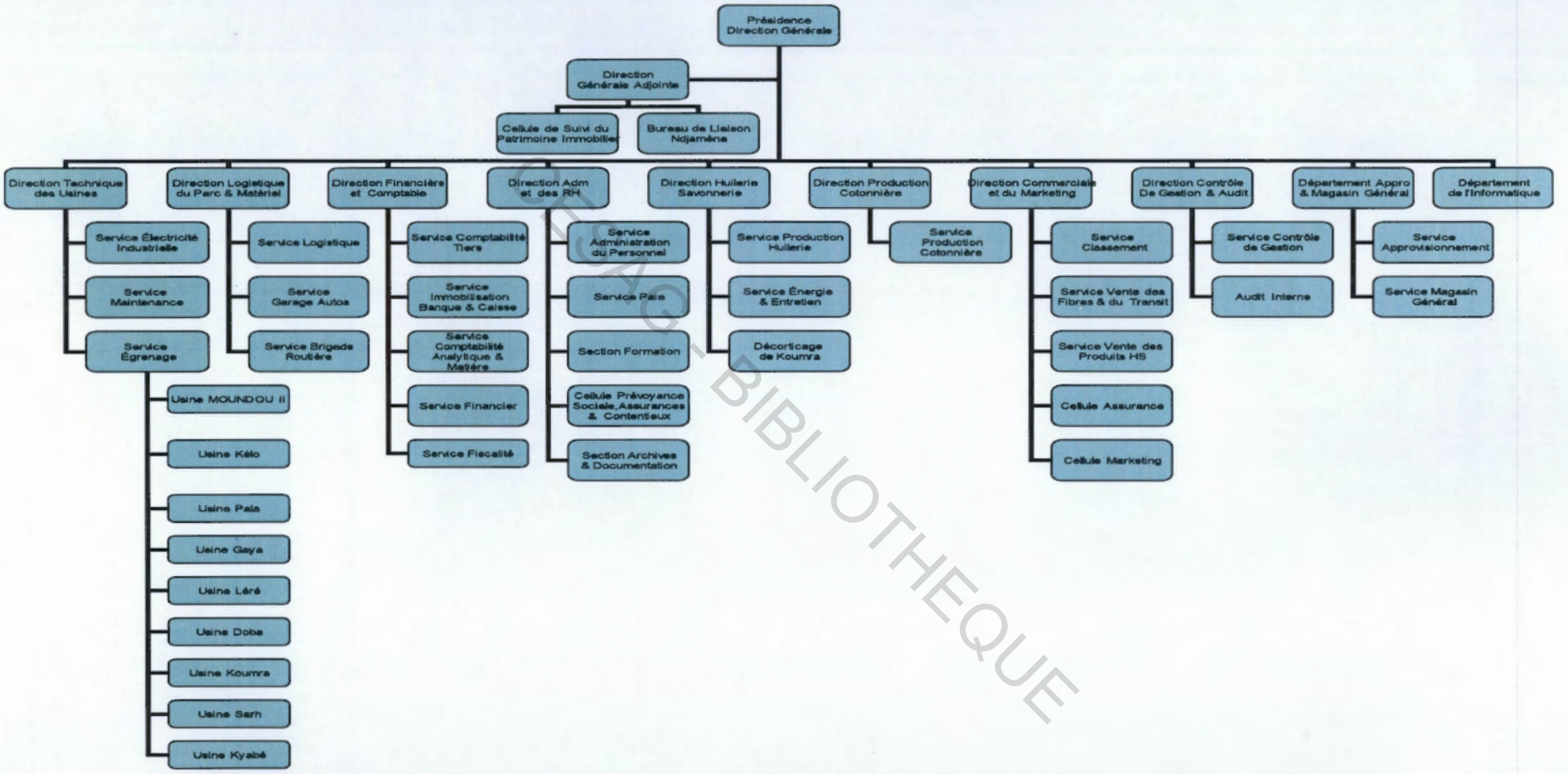
Source: COTONTCHAD, Direction Administrative et des Ressources Humaines (DARH)

1.4. Evolution du Chiffre d'Affaires (CA/HT) et du résultat net des cinq dernières années

	2007	2008	2009	2010	2011
CA global HT (en millier)	49 718 040	30 188 746	23 725 876	24 698 006	32 518 905
Résultat Net (en millier)	-6 017 304	-1 880 977	-6 048 157	5 687 739	3 562 435

Source: Etats financiers au 31/12/2011, Direction Financière et Comptable (DFC).

ANNEXE 2: organigramme actuel de la COTONTCHAD.



Source: COTONTCHAD, Direction Administrative et des Ressources Humaines (DARH).

ANNEXE 3: situation des matériels informatiques de la COTONTCHAD

3.1: Récapitulatif des micros ordinateurs et imprimantes de la COTONTCHAD

Direction / Département	Bon Eta		Etat Moyen		Vétustes et/ou en panne	
	Micro	Imprimante	Micro	Imprimante	Micro	Imprimante
DAMG	10	9	6	1	1	0
DARH	7	5	4	0	4	0
DCM	4	4	1	0	3	0
DCGA	7	4	0	0	0	0
DFC	24	15	4	0	4	0
DHS	7	6	2	1	8	3
DI	6	1	1	1	3	0
DPLM	4	2	0	0	0	1
DPC	4	2	1	0	1	0
DTU	8	13	7	0	6	0
PDG	3	3	0	0	0	0
TOTAL	**84**	**64**	**26**	**3**	**30**	**4**

Total Micros = 140

Total Imprimantes = 71

Source: Département Informatique: Etat d'inventaire des matériels informatiques.

DAMG: Département Approvisionnement et Magasin Général.

DARH: Direction Administrative et des Ressources Humaines

DCM: Direction Commerciale et marketing

DCGA: Direction du Contrôle de Gestion et audit

DFC: Direction Financière et comptable

DHS: Direction Huilerie Savonnerie

DI: Direction Informatique

DPLM: Direction du Parc, de la Logistique et du matériel

DPC: Direction de la production Cotonnière

DTU: Direction Technique des Usines

PDG: Présidence Direction Générale.

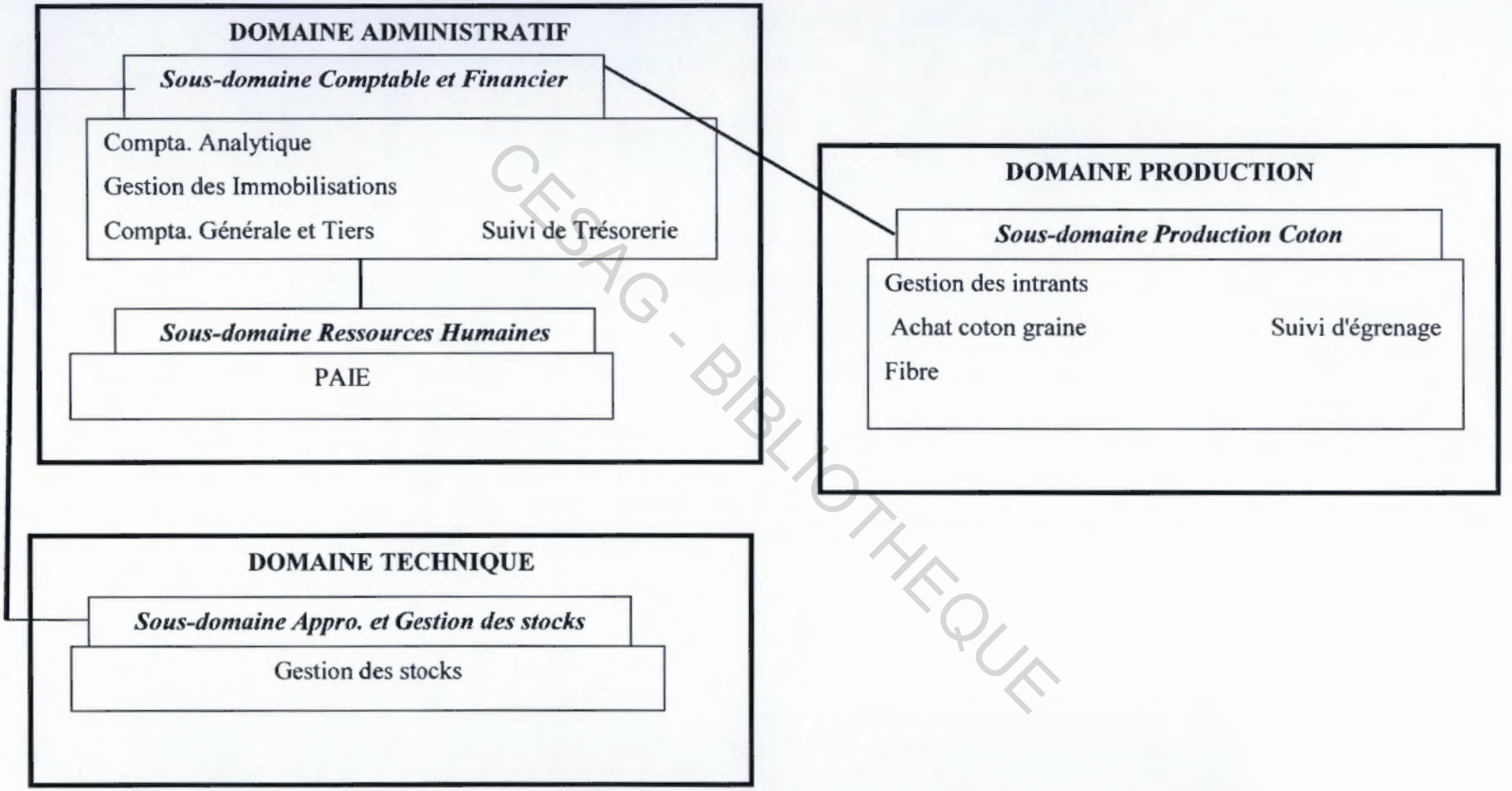
3.2: Récapitulatif des matériels du Département Informatique

Matériel inform.	Type	Rôle	Qté	Date MES
Micro ordinateur	HP Proliant 350	Serveur	2	2009 et 2010
Micro ordinateur	Portable	Poste de travail mobil	2	2010
Micro ordinateur	Compact 5008 MT	Poste de travail bureau	1	2010
Micro ordinateur	HP d220/530	Poste de travail bureau	2	2005/2007
Micro ordinateur	Compact EVO	Poste de travail bureau	3	2002/2007
Imprimante	HP Laserjet 4	Impression des documents	2	2000/2007
MODEM		Télécommunication	7	
ROUTEURS		Connexion des sous-réseaux	2	
SWITCH		Regroupement des lignes	17	
VSAT		Connexion satellitaire	7	

MES: Mise En Service

Source: Nous même, à partir des Etats d'inventaire du département Informatique

ANNEXE 4: cartographie des applications informatiques - Schéma général



Source: Nous même, adapté du Schéma directeur informatique (1992).

ANNEXE 5: Guide d'entretien avec le Responsable informatique

1 Revue générale des processus

1.1. Acquisition et développement des applications (solutions) informatiques.

- Comment sont achetées ou développées les applications ou solutions informatiques?
- Comment sont installés et validés les nouveaux systèmes informatiques?
- Comment est assurée la maintenance des systèmes d'information?

1.2. Distribution et support informatique

- Quelle est la qualité du support fourni aux utilisateurs?
- Comment sont gérés les problèmes d'exploitation quotidiens?
- Comment sont gérées les fonctions externalisées?

1.3. Gestion de la sécurité et continuité de l'exploitation

- Comment sont gérées les sauvegardes, Existe-t-il un plan de secours?
- Comment est définie et mise en œuvre la sécurité logique?
- La sécurité physique est-elle satisfaisante?

ANNEXE 6: Synthèse des points forts et des points faibles des processus informatiques et applicatifs

PROCESSUS / SOUS-PROCESSUS	POINTS FAIBLES	POINTS FORTS
1. Les processus informatiques *1.1. La fonction informatique* *1.1.1. L'organisation interne de la fonction*	- Absence d'organigramme. - Absence de description des postes. - Non séparation des fonctions/tâches. - Absence d'un schéma directeur informatique (SDI)/Plan stratégique. -Absence de cartographie des risques informatiques et de revue de l'audit interne. - Absence des procédures formalisées	- Passage de la structure de service à celle de département. - Rattachement à la Présidence-Direction Générale. - Participation du responsable au Comité de Direction (CODIR).
1.1.2. Les compétences informatiques	- Insuffisance des compétences / unicité de compétence; - Insuffisance de formation continue des agents; - Faible motivation des collaborateurs.	- Expérience et ancienneté reconnue du responsable du département: -Interlocuteur direct de la Direction Générale.
1.2. Les étude et développement	- Absence de méthodologie de développement et gestion des projets; - Absence de tableaux de bord, d'outils de suivi et d'évolution des développements; - Inadéquation des méthodes, des techniques et des outils utilisés; - Formation insuffisante des utilisateurs -Documentation inexistante ou insuffisante - Analyse insuffisante dans la phase des études et conception; - Evolution très lent des développements.	- Maintenance des applications opérationnelles par le responsable et un collaborateur.
1.3. Mise en service des applications et exploitation informatiques	- Absence de procédures formalisées de gestion de l'exploitation informatique; - Tests exécutés sans le recours à une méthodologie appropriée;	

	- Absence de registre de suivi des incidents informatique; - Absence d'outil de suivi de performance du réseau - Absence de séparation des tâches entre études et exploitation; - Documentation technique inexistante ou insuffisante; - Absence d'interfaces automatiques entre les applications; - Absence de tableaux de bord et d'outils de suivi de l'exploitation.	
1.4. Maintenance *1.4.1. Maintenance des matériels*	- Insuffisance de maintenances préventives; - Bugs à répétition; - Maintenance générique non définie. - Absence de définition du champ d'application de la maintenance; - Absence de tableaux de bord de bord de performance du service - Salles machine vétustes.	- Existence d'un Service Maintenance; - Procédures de maintenance formalisées et appliquées. - Climatisation des salles machine satisfaisante;
1.4.2. Maintenance des applications	- Absence d'évolution ou évolution très lente des applications; - Absence d'interface entre applications; - Bugs à répétition	- Maintenance assez satisfaisante; - Interface de l'application "Gestion des IMMO avec la COMPTA."
1.5. Sécurité et continuité de l'exploitation *1.5.1 Gestion des risques informatiques*	- Absence de procédures d'analyse et d'évaluation des risques informatiques; - Absence de cartographie des risques informatiques; - Non de sensibilisation des utilisateurs et autres acteurs aux risques informatiques. - Absence de plan et mesures de sécurité relatives aux infrastructures et applications; - Absence de mise à jour ou mise à jour irrégulière d'anti virus sur les serveurs et les postes de travail.	

1.5.2. Sécurité physique	- Absence de politique de sécurité bien définie et connue; - Insuffisance des moyens adéquats de protection des ressources informatiques contre les pirates, les virus, les pannes électriques, la fraude, malveillance etc. - Absence ou insuffisance des contrôles des accès physiques aux locaux et ressources	- Climatisation satisfaisante des salles machine; - Extincteurs; - Onduleurs; - Agents de sécurité et gardiennage.
1.5.3. Sécurité logique	- Absence de politique formalisée de sécurité logique; - Absence de séparation de fonction; - Absence de mise à jour des listes des personnes autorisées à accéder aux systèmes informatiques; - Absence de procédures formalisées de mise à jour d'antivirus sur les postes de travail des utilisateurs; - Accès au système d'information non contrôlé - Non règlementation de l'accès à l'internet, messagerie et utilisation des clés USB.	
1.5.4. Plan de continuité: - *Sauvegardes* - *Assurance*	- Sauvegardes effectuées non stockées en lieux sûrs ou hors site d'exploitation; - Absence des tests de reprise des sauvegardes; - Absence de tests sur le temps nécessaire pour redémarrer le système en cas d'incident ou sinistre avéré; - Absence de plan de reprise défini et documenté; - Absence de tests de reprise d'activité en cas d'incident	- Assurance complète du parc informatique
1.6. Assistance aux utilisateurs	- Formation insuffisantes des utilisateurs à l'utilisation des ressources informatiques - Absence de charte des utilisateurs du système d'information - Absence d'un service support aux utilisateurs (helpdesk) - Non implication des utilisateurs aux processus d'acquisition ou de développement des ressources informatiques.	

2. Les processus d'application		
Contrôle d'accès aux applications	- Absence de procédures formalisées d'accès aux ressources logiques; - Absence de mis à jour des mots de passe et de changement périodique; - Existence des profils ou comptes génériques des utilisateurs au sein des applications.	Existence des listes des utilisateurs habiletés.
Contrôle de la collecte et la saisie des données	- Absence des procédures écrites des collectes et saisies des données	- Existence des pratiques de collectes et saisies des données régulièrement mises en ouvre
Contrôle de l'enregistrement des données	- Erreurs de saisie; - Double saisie; - Mauvaises manipulation des données à l'enregistrement.	- Vérification et validation des données avant enregistrement; - Rapprochement des données enregistrées des états édités.
Contrôle des traitements et des sorties des données	- Interface manuel des applications; - Absence de certains contrôles sur des données issues des traitements; - Insuffisance des contrôles des anomalies relevées; - Absence de recyclage des données rejetées.	- Rapprochement des données sorties avec les états manuscrits: - Recoupement avec d'autres sources de saisie.
Les contrôles sur les interfaces d'application - *Qualité des interfaces* - *Niveau de stabilisation* - *Mode de traitement des anomalies*	- La plupart des interfaces sont manuels; - L'interface automatique génère parfois des anomalies; - Les états d'anomalie ne sont parfois pas correctement analysés.	- Correction des anomalies constatées; - modification des programmes toujours à la demande des utilisateurs

ANNEXE 7: Questionnaire d'évaluation de contrôle interne (QCI)

QUESTIONNAIRE DE CONTROLE INTERNE.

OBJECTIS RECHERHES:

1. Organisation de la fonction informatique:

- s'assurer que la fonction informatique dispose d'une structure efficace permettant une bonne séparation des tâches

2 **Exploitation informatique:**

- s'assurer que les opérations d'exploitation sont correctement définies, planifiées et suivies;

3. **Développement des applications:**

- s'assurer que les procédures de développement et de modification des programmes sont correctement définies, autorisées et appliquées;

4. Sécurité:

- s'assurer que les accès aux données et aux transactions sont correctement autorisés;

5. Plan de secours et les sauvegardes :

- s'assurer que des mesures ont été mises en place afin d'assurer la restauration du système d'information en cas de sinistre informatique

ORGANISATION INFORMATIQUE ET DES SYSTEMES D'INFORMATION.

I. Structure Organisationnelle et Existence d'un plan informatique.

1. STRUCTURE ORGANISATIONNELLE

- ***Organisation de la fonction informatique***

QUESTIONS	*Oui*	*Non*	*Observations*
• Quelle est la structure organisationnelle en charge de l'informatique (et des systèmes d'information) au niveau la *Cotontchad*?	X		Département Informatique
• A qui est rattachée cette structure ?	X		Direction générale X

• Quel est son statut au niveau de l'organigramme (Direction, Division, Service) ?			**Bonne communication**
• Quelle est la relation entre la plus haute instance de *la société*, la structure SI et les structures métiers et supports de *la société* ?			**X**
• Cette *Direction (DI)* est-elle organisée en plusieurs divisions ou services ?	X		**N/A**
- Lister ces entités ou services et leurs effectifs.			
- Décrire brièvement les responsabilités, missions et attributions de la *Direction Informatique* ?	X		
- Les missions et responsabilités de la *Direction Informatique*, sont-elles explicites et claires ?			
• Existe-t-il un document officiel (fiche de fonction) fixant les attributions et les missions de chaque entité (service) rattachée à *la Direction Informatique?*		**X**	
- Si la réponse à cette question est négative, expliquer comment est défini le champ d'intervention de *la Direction Informatique*?		**X**	
• Ces fiches de fonction sont-elles diffusées aux différents responsables de *la Direction Informatique*?		**X**	
• Ces fiches de fonctions (ou autre document similaire) sont-elles connu de tous les acteurs de la *Direction Informatique*?			
- Si la réponse à cette question est négative, argumenter et expliquer			

• Quel est l'effectif alloué à la *Direction Informatique* ?	**X**		**3 AGENTS**
cet effectif vous parait-il suffisant eu égard les missions qui sont définies au niveau des fiches de fonction ?		**X**	

• Le personnel alloué à la *Direction Informatique* possède-t-il les compétences techniques requises, lui permettant de réussir au mieux ses missions et responsabilités :	**X**		
- Très bonne connaissance de la société et de ses activités	**X**		**BONNE**
- Très bonne connaissance de la réglementation en vigueur		**X**	
- Maitrise des procédures de gestion en vigueur		**X**	
- Maîtrise des architectures informatiques et des outils informatiques (système de base de données, etc.)	**X**		
- Maîtrise des techniques de conception, de développement, de test des applications informatiques,		**X**	

- Maîtrise de la méthode de conduite de projet et les outils associés, - Savoir anticiper les difficultés et agir, - Savoir gérer des projets complexes, - Savoir communiquer et négocier avec les autres structures de *la société*	X X X	X	
• Le personnel informatique suit-il des actions de formations de mise à niveau pour accompagner le développement des systèmes d'information ? - Si la réponse à cette question est positive, décrire les actions de formation qui ont été menées et leurs relations avec les activités *de la Direction Informatique* - Si la réponse à cette question est négative, argumenter et expliquer (est-ce lié à une problématique de budget)	X		
• Quels sont les différents matériels, logiciels et supports utilisés par le système d'information ? - Identifier les principales architectures techniques (composantes réseau télécom) - Donner la liste des matériels et logiciels informatiques existant au niveau de la *société Cotontchad.* - Sont-ils tous opérationnels ? ou nouvellement développés ?	X X X		
• Existe-t-il des documentations utilisateurs et de gestion des différentes applications informatiques ? • Ces documentations utilisateurs, sont-elles mises à disposition de toutes les entités qui utilisent les applications informatiques ?	X X		**PARTIELLEMENT**

2. EXISTENCE D'UN PLAN INFORMATIQUE.

QUESTIONS	*OUI*	*NON*	*OBSERVATIONS*
• La *société Cotontchad* dispose-t-elle d'un plan informatique stratégique ou d'un schéma directeur à long terme ?		X	
• Ce plan informatique ou schéma directeur informatique comporte-t-il toutes les informations relatives au budget dédié à l'informatique, aux domaines d'activité couverts, aux effectifs alloués à l'informatique, aux moyens de sécurité et de sauvegarde des données, aux technologies d'information utilisées et celles prévisionnelles, aux projets en cours et ceux prévus, …) ?		X X	

• Si la réponse à cette question est oui, ce schéma directeur à long terme, est-il esquissé régulièrement en plans informatiques à court terme (annuels)? • Le plan informatique ou le schéma directeur décline–t-il les objectifs à court et moyen termes (les décrire succinctement).		X	
• Le plan informatique ou schéma directeur couvre-t-il tous les domaines de gestion de la *société Cotontchad* (activités support et activités opérationnelles)? - Enumérer les domaines couverts, les bases de données et les applications correspondantes.		X X	
• Le schéma directeur comporte-il un descriptif de la politique générale et des orientations stratégiques en matière de management des systèmes d'information de *la société*?		X	
• Le schéma directeur comprend-t-il : - Un descriptif fonctionnel de chaque domaine d'activité identifié (activités opérationnelles et activités support) - Une étude de faisabilité permettant de prévoir les moyens humains, matériels et logiciels nécessaires à la mise en œuvre des actions définies dans l'étude fonctionnelle ?		X X X	
• Les plans informatiques à court et moyen termes sont-ils diffusés aux gestionnaires et utilisateurs futurs concernés dans la société?		X	
• Le plan informatique à court terme prend-il en considération les modifications organisationnelles, les évolutions technologiques et les exigences de la réglementation en matière de technologies de l'information ?		X	
• Les plans informatiques à long et court terme sont-ils régulièrement actualisés pour les adapter aux évolutions technologiques ?		X	
• Le schéma directeur prévoit-il une documentation appropriée qui sert de support aux projets informatiques ?		X	
• La société a-t-elle mis en place des points de contrôle pour s'assurer que les objectifs et les plans à long et court terme informatiques sont toujours conformes aux objectifs et aux plans stratégiques à long et court terme de la société ?		X	
• Est-ce que les propriétaires des processus et l'encadrement supérieur effectuent une revue des plans informatiques et donnent leur approbation ?		X	

• *La Direction Informatique* tient-elle, au moins deux fois par an, des réunions avec le comité directeur pour contrôler l'application du schéma directeur et des plans informatiques à court terme et les réviser si nécessaire ?		X	
• Le plan informatique à long terme est-il modifié régulièrement pour l'adapter en fonction des modifications qui interviennent dans le plan stratégique à long terme de la société et des changements des technologies de l'information ?		X	

3. ARCHITECTURE FONCTIONNELLE.

- *Définition de l'architecture fonctionnelle.*

QUESTIONS	*OUI*	*NON*	*OBSERVATIONS*
• Décrire l'architecture fonctionnelle des systèmes d'information ?	X		
• Cette architecture répond elle aux besoins des utilisateurs ?	X		
• Quels sont les domaines d'activité couverts par l'informatique ?	X		**cf. schéma descriptif**
• Pour chaque sous système d'information, - Décrire l'existant et identifier les contraintes techniques de confidentialité et de validité sur les données. - Décrire les schémas de circulation d'information et les moyens utilisés pour les échanges de données. - Quels sont les inputs de chaque sous système d'information ? - Quels sont les outputs de chaque sous système d'information ? Ces outputs sont-ils adaptés et répondent-ils aux besoins et attentes des utilisateurs ? - Si la réponse à cette question est négative, décrire les besoins des utilisateurs en termes d'output ? - Quels sont les moyens techniques mis à la disposition du système d'information ? - Quels sont les acteurs du système d'information ?	X X X X X X X X		**tous les services**
• Quel est le niveau d'automatisation du Système d'Information?	X		
• Quels sont les traitements automatisés du système d'information ?	X X		

• Recenser les applications informatiques et leurs fonctionnalités ? Ces applications informatiques sont-elles intégrées ? Cf. Rubrique suivante.	X		
• Quels sont les traitements non automatisés du système d'information (les procédures et les règles de gestion sont-elles formalisées) ? • Ces procédures et règles de gestion sont-elles diffusées et communiquées à l'ensemble des acteurs concernés ?		X	**- Commercial** **- Pilotage**

4. APPLICATIONS INFORMATIQUES.

- *Applications informatiques.*

QUESTIONS	*OUI*	*NON*	*OBSERVATIONS*
• Identifier, recenser et lister toutes les applications informatiques opérationnelles au niveau de la *société*.	X		**CF. Listing et description**
• Parmi ces applications, faire la distinction entre les applications qui ont été développées en interne, et celles qui ont été acquises ? • Comment est opéré le choix de l'une ou l'autre option et quels sont les critères qui sont pris en compte ? • Pour les applications développées en interne, a-t-il été élaboré un cahier des charges définissant les besoins fonctionnels des utilisateurs ? • Décrire la procédure suivie pour l'acquisition de solutions informatiques. • Dans les cas où la solution informatique a été acquise, existe-t-il un contrat de service ? Les utilisateurs ont-ils été formés au produit et ont-ils été assistés pour son paramétrage ? • Le paramétrage a-t-il été réalisé dans les règles de l'art ?	X X X X X X X		
• Existe-t-il, pour chaque application, un document décrivant l'analyse fonctionnelle et les besoins des utilisateurs ? • Décrire, pour chaque application informatique, les principales fonctionnalités et leur degré de réponse aux besoins des utilisateurs ?	X		
• Est-il opéré un contrôle de la fiabilité des données et leur degré de réponse aux attentes et besoins des utilisateurs ?			

• Ce contrôle, se base-t-il sur : - des entretiens avec le personnel informatique ainsi qu'avec certains utilisateurs ? - des contrôles de documents ou d'états pour la validation des réponses ?			
• Pour chaque application informatique, existe-t-il une documentation utilisateur, un dossier d'exploitation, et un dossier de maintenance ? Ces documentations sont-elles régulièrement mises à jour en cas de changement de versements et sont-elles conservées en lieu sûr ? • Cette documentation est-elle communiquée aux utilisateurs concernés ?	X X X		
• Cette documentation est-elle de qualité et est-elle facilement compréhensible ? • Cette documentation prévoit-elle des illustrations des différents écrans de saisies et écrans de sorties ? Toutes les rubriques sont elles bien expliquées ?	X X X		
• Les accès aux applications informatiques sont-ils sécurisés ?	X		
• Les applications informatiques sont-elles évolutives ? Sont-elles mises à jour régulièrement (dès que les procédures ou réglementations changent, les données en entrées ou en sorties ont été modifiées) ?	X X		
• Ces évolutions, modifications et mises à jour sont-elles reprises dans des documents utilisateurs ?	X		
• Les procédures de contrôle et d'autorisations des accès sont-elles formalisées et connues de tous ?	X		
La politique de sauvegarde est-elle connue de tous ? est-elle appliquée ? • Quelle est la périodicité des sauvegardes informatiques ? • Des contrôles de sauvegarde sont-ils régulièrement réalisés ? • Ces sauvegardes informatiques sont-elles rangées en lieu sur ?	 X X	X	 **Quotidienne** X

5. . ACQUISITION ET MISE EN PLACE.

- *Sécurité Informatique :*

Politique de sécurité de la société.

QUESTIONS	*OUI*	*NON*	*OBSERVATIONS*
• La politique de sécurité informatique (physique et logique) est-elle formalisée au niveau de *la société ?*		X	
• *La Direction Informatique* a-t-elle élaboré un document officiel ou charte sur la sécurité qui décline cette politique en actions et procédures concrètes ?		X	
• Est-il désigné, pour des raisons d'efficacité au niveau de la société un correspondant de la sécurité informatique qui a une vision globale (aspects physiques et aspects logiques) de la société ainsi que de l'environnement informatique, afin : - de pouvoir détecter des incohérences notoires, et donc de proposer si nécessaire des évolutions, - de veiller, en relation avec les autres administrateurs à l'application des règles, - pouvoir coordonner les actions de «riposte» en cas d'incident, ***N.B :*** *Par aspects physiques, on entend la protection contre le vol, l'incendie, les inondations, protection des accès physique, protection des supports de données (sauvegardes) etc.,* *Par aspects logiques/logistiques, on fait référence aux contrôles d'accès par mots de passe (complexité, périodicité, etc.), aux actions de sensibilisation, formations, etc.*		X	
• Cette charte (*la politique de sécurité)* ou document officiel sur la sécurité informatique a-telle été entérinée par l'ensemble des instances de la société?		X	
• Cette charte ou document officiel sur la sécurité est-elle diffusée à tous les utilisateurs de l'informatique ?		X	
est-elle respectée et appliquée ?		X	
• Des séances de formation et/ou de sensibilisation sont-elles organisées dans ce cadre ?		X	
• Cette charte prévoit-elle des mesures de sanctions à l'égard des personnes qui l'enfreignent ?			

Sécurité physique et accès aux locaux informatiques

• Est-il procédé à une identification de l'ensemble des risques et menaces en relation avec la sécurité physique des données et équipements		X	

informatiques (accès aux locaux d'exploitation, protection physique des équipements, mesures de sécurité contre les intempéries, incendies, …) ?		X	
• Cette liste des risques et menaces est-elle connue par tous les utilisateurs de l'informatique et des systèmes d'information ?		X	
• Pour faire face, a-t-il été établi une matrice des solutions et actions à entreprendre pour contrer chacun des risques identifiés (Plan de reprise en cas d'incident)?		X	**Liste à établir**
• Y a-t-il des risques qui ne sont pas couverts ?			
• Si la réponse à cette question est positive, établissez la liste de ces risques non couverts et argumenter pourquoi il n'a pas été identifiés pour eux des solutions et/ou actions à entreprendre pour les contrer ou les réduire ?			

Sécurité physique des locaux informatiques.

• La procédure de sécurité physique est-elle formalisée, diffusée et connue de tous ?		X	
- Décrire comment sont sécurisées les infrastructures matérielles informatiques de type serveurs et autres (salles sécurisées, lieux ouverts au public, espaces communs au niveau de la société),		X	
- Décrire comment sont sécurisés les postes de travail des personnels qui sont en accès libre :	X		
- contre l'accès de personnes étrangères ou autres (mot de passe et authentification, badges pour les visiteurs, verrouillage de sessions, mises sous clés pour les postes sensibles…),	X		
- contre le vol (procédure de gestion des entrées et sorties des équipements informatiques, verrouillage, câbles antivol pour les portables, …)	X		
- contre les virus (procédures de détection des virus)	X		
- Identifier et lister les pannes techniques et/ou incidents les plus récurrentes puis en analyser les causes,		X	
- Est-il prévu une procédure de simulation de gestion des pannes techniques (cas extrêmes) ?		X	
- Est-il établi, au niveau de *la société*, un recueil de suivi de toutes les pannes ou incidents techniques ?		X	
- Des tableaux de bords sur la gestion des risques techniques sont-ils élabores afin d'assurer le suivi de ces risques ?		X	

Sécurité logique des données informatiques

• L'accès aux locaux abritant le matériel informatique (serveurs et autres) est-il limité aux seuls administrateurs du système informatique ?		X	
• La procédure de sécurité logique des données est-elle formalisée, connue et appliquée par tous les acteurs concernés de la société ?		X	
• Décrire succinctement les grandes lignes de cette procédure ?			
• Cette procédure de sécurité logique des données permet-elle de couvrir les trois objectifs suivants			
- **L'intégrité** des données,	X		
- **La confidentialité**, consistant à assurer que seules les personnes autorisées ont accès aux ressources,			
- **La disponibilité**, permettant de maintenir le bon fonctionnement du système informatique			
• Si cette procédure n'est pas formalisée, essayer de dégager (au vu des entretiens) avec le responsables informatique les modalités de gestion de la sécurité des données informatiques.		X	
• Est-il établi une liste des risques et menaces relatives à la gestion des données, encourus par *la société* ?		X	
• Est-il établi une matrice des solutions et actions à entreprendre pour contrer ces risques et menaces ?			
• Les procédures d'autorisation aux ressources dont Internet sont-elles limitées et contrôlées ?	X		
• Des sessions de formation et de sensibilisation sont-elles organisées au profit du personnel dans ce cadre ?		X	
• Comment est gérée la protection des données ?			
- Est-il formalisée une procédure d'Identification / Authentification pour protéger les données contre des accès frauduleux ou malveillants aux ordinateurs de *la société*		X	
- Est-il formalisée une procédure de Sauvegarde / Restauration pour conserver les données sensibles en sécurité afin de les restaurer en cas de sinistre (erreur humaine, incendie, virus, etc.) procédure de contrôle des accès, procédures de sauvegarde et de restauration des données ?		X	X
• Le système de stockage et de sauvegarde des données est-			

il évolutif ?			

6. DEVELOPPEMENT DES APPLICATIONS INFORMATIQUES.

- ***Développement des applications informatiques.***

QUESTIONS	*OUI*	*NON*	*OBSERVATIONS*
• Etablir la liste de toutes les applications et projets développés pour répondre à des besoins spécifiques de *la société* ?	X		
s'agit-il de grands projets ou de petits projets de types bases de données ?	X		
• Ces opérations s'inscrivent-elles dans le cadre du plan informatique ?	X		
• S'agit-il de développements en interne (réalisés par la structure informatique) ou en externe (par des prestataires de services)?	X		
• Ces développements ont-ils fait l'objet d'une analyse conceptuelle, fonctionnelle et organique, permettant d'identifier et de recenser tous les besoins fonctionnels, les inputs ainsi que les outputs, les contrôles à mettre en place, les limitations d'accès, …		X	Quelques enquêtes auprès des utilisateurs
• Décrire la démarche généralement adoptée et mettre en évidence les éventuels dysfonctionnements.		X	
• Des tests ont-ils été opérés avant d'opérer la migration des données vers les nouvelles applications ?	X		
• Ces tests et jeux d'essais ont-ils donné entière satisfaction aux utilisateurs concernés ?	X		
Les documentations utilisateurs et documentations d'exploitation sont-elles disponibles et diffusés aux acteurs concernés ?		X	
Est-il prévu un contrat de maintenance pour assurer les éventuelles modifications ainsi que gérer les éventuels problèmes qui peuvent survenir ?	X		

7. MAINTENANCE ET EXPLOITATION

- ***Maintenance du matériel informatique.***

QUESTIONS	*OUI*	*NON*	*OBSERVATIONS*
• Les procédures et modalités de gestion des opérations de maintenance sont-elles formalisées dans un document officiel connu par tous ?	X		
• La maintenance des applications informatiques et équipements informatique est-elle assurée par la fonction		X	- partiellement

informatique ou est-elle sous-traitée aux prestataires de services moyennant des contrats de maintenance ?			**Assurée par un autre service interne**
• Comment sont gérées les actions de maintenances des applications et équipements informatiques ? • Est-il établi, pour chaque panne, incidents, modification, ou autre, une demande d'intervention spécifique ? • Cette demande d'intervention est-elle signée par le responsable hiérarchique direct du demandeur ?X	X X X		**Procédures non es**
• Quel est le circuit de cette demande d'intervention ? Par qui sont centralisées toutes les demandes d'interventions ? • Ces demandes d'intervention sont-elles examinées, triées par type d'intervention puis classées par niveau de priorité ? • Quel est le délai moyen pour donner suite à une demande d'intervention ? • Arrive-t-il qu'il y ait des relances ? Ces relances sont-elles formalisées ?	X X		**CF. Procédures fois longues**
• Une fois que le problème est réglé, l'état des demandes d'intervention est-il mis à jour ?		X	
• Est-il établi un tableau de bord pour le suivi des anomalies et problèmes signalés et leur évolution ?		X	
• Est-il établi des statistiques sur les types d'anomalies qui surviennent fréquemment ? est-il réalisé une analyse des causes de ces pannes, incidents ou anomalies (formation des utilisateurs insuffisantes, qualité du matériel, virus, …)		X X	

8. CONTROLE ET SUIVI INFORMATIQUE.

- ***Suivi et contrôle du système d'information.***

QUESTIONS	*OUI*	*NON*	*OBSERVATIONS*
• Assure-t-on un suivi fréquent du fonctionnement, des coûts, du respect du calendrier et des éléments de sécurité et de fiabilité du système d'information ?		X	
• Procède-t-on périodiquement à des examens auprès des utilisateurs du système d'information afin de suivre les progrès réalisés et de déceler les problèmes éventuels ?		X	
• Est-ce que des examens sont effectués aux points de contrôle importants avec les utilisateurs afin d'examiner les outputs du système d'information et les différents circuits ?		X	**Sauf s'il ya plainte**

• Les problèmes et les questions techniques sont-ils identifiés, documentés et font-ils l'objet d'un suivi ?		X	
Existe-t-il une procédure, un mécanisme ou des seuils d'alerte pour assurer le suivi des altérations ou obsolescences pouvant affecter le système d'information notamment à cause du progrès technique ?		X	
• La haute direction fournit-elle un appui, des ressources et des fonds suffisants pour assurer de l'efficacité du Système d'Information ?	X		
• Le système d'information est-il doté de points de vérification, de sorte que les *auditeurs (internes) ou* inspecteurs puissent faire son suivi et se prononcer relativement à son fonctionnement et prendre les corrections qui s'imposent ?		X	
• A-t-on les éléments permettant de dire à quel moment il faudrait prévoir les points de contrôle ?		X	
• Dispose-t-on des éléments relatifs aux critères de bon fonctionnement du système d'information ?		X	
• Est-ce que les risques affectant le système d'information sont définis, évalués et documentés ?		X	
• Une démarche de gestion des risques a-t-elle été engagée dans ce cadre ? • Si la réponse à cette question est négative, décrire la procédure en vigueur.		X	

9. SATISFACTION DES UTILISATEURS.

- ***Satisfaction des utilisateurs.***

QUESTIONS	*OUI*	*NON*	*OBSERVATIONS*
• Le responsable du système d'information a-t-il prévu que tous les utilisateurs soient représentés dans le système d'information, de manière à ce que chaque groupe d'utilisateurs puisse participer à la définition des besoins, à la conception du système et à sa mise en œuvre ?		X	
• Les destinataires ont-ils été informés précisément de ce que le système va leur fournir, de l'interaction qu'ils pourront avoir avec le système et de la possibilité qu'ils auront de proposer des améliorations ?		X	
• Les utilisateurs ont-ils officiellement la possibilité de contribuer aux examens et mises à jour du système d'information en fonctions de leurs attentes ?	X		
• Le système d'information s'adresse-t-il aux divers utilisateurs et permet-il de répondre aux attentes de chacun ?	X		

• De quelles informations les utilisateurs ont-ils besoin ?			
• Quels sont les indicateurs et/ ou les ratios clés sur lesquels les utilisateurs doivent se pencher et suivre l'évolution pour mener à bien leur mission ?			
De quelles autres informations les utilisateurs doivent-t-ils disposer pour être bien informés sur les éléments qui les intéressent ?			
• De quelle manière ces documents doivent-t-ils être conçus pour répondre aux besoins des différents utilisateurs ?			
• A quelle fréquence et avec quelle rapidité les utilisateurs peuvent-ils recevoir l'information ?			
• De quelle manière les besoins des utilisateurs évolueront-t-ils à l'avenir et de quelle manière cette évolution influera-t-elle sur la conception du système d'information ?			

BIBLIOGRAPHIE

OUVRAGES et ARTICLES GENERAUX

1. **ACISSI (2009)**, Sécurité informatique: Ethical hacking, apprendre l'attaque pour mieux se défendre, Editions ENI, Paris, 355 Pages.
2. **AFAI (2008)**, Guide d'audit des systèmes d'information: Utilisation de Cobit, IT, Gouvernance Institute, Paris, 269 Pages.
3. **AMF (2010),** Les dispositifs de gestion des risques et de contrôle interne. cadre de référence. Paris, 36 Pages.
4. **AMF (2007),** Le dispositif de contrôle interne: cadre de référence. Paris, 65 Pages.
5. **ANGOT Hugues (2004)**, Audit comptables, audit informatique, 3ème 2dition de BOECK, Paris, 299 Pages.
6. **BARRY Mamadou (2009)**, Audit et contrôle interne, DAKAR, 370 Pages.
7. **BARTHELEMY Bernard & COURREGES Philippe (2004)**, Gestion des risques : Méthodes d'optimisation globale, 2è édition. Edition d'organisation, 472 pages.
8. **BERTIN Elisabeth (2007)**, Audit interne. Enjeux et pratique internationale. Les Editions d'Organisation, Paris, 318 Pages.
9. **BUTEL Annie (2008)**, Continuité d'activité: Plan de secours, CLUSIF / BNP PARISBAS, Paris, 33 Pages.
10. **CARPENTIER Jean-François (2009)**, la sécurité informatique dans la petite entreprise: état de l'art et bonnes pratiques, Editions ENI, Paris, 277 Pages.
11. **CLEARY Sean & MALLERET Thierry (2006)**, Risques : Perception Evaluation Gestion. Edition Maxima, 253 pages
12. **COTONTCHAD (1992)**, Schéma directeur informatique, SEDES-CEGOS SA, N'Djamena, 154 Pages.
13. **COURTOT Hervé (1998)**, La gestion des risques dans les projets, ECONOMICA, Paris 224 Pages.
14. **DAYAN Armand et Al. (2008)**, Manuel de gestion Vol.1, 2ème édition, ELLIPSE/AUF, Paris, 1088 Pages.
15. **DERIEN Yann (1992)**, Les techniques de l'audit informatiques, DUNOD, Paris, 238 Pages.
16. **DESMOULINS Nicolas (2009)**, Maîtriser le levier informatique: accroître la valeur ajoutée des systèmes d'information. Edition Pearson Education, Paris, 259 Pages.
17. **DESROCHES Alain et Al. (2003)**, La gestion des risques, Edition LAVOISIER, Paris, 285 Pages.

18. **GHERNAOUITI-HELIE Solange (2011)**, Sécurité informatique et réseaux, DUNOD 3ème Edition, Paris, 368 Pages.
19. **GILLET Patrick et Michelle (2008)**, Management des systèmes d'information, DUNOD, Paris, 443 Pages.
20. **GODART Didier (2002)**, Sécurité informatique: risque, stratégies, solutions, EDIPRO, Paris, 334 Pages.
21. **GRAEVE Jean et POTIER Jean (2001)**, Système d'information, Management et Acteurs, Les éditions SAPIENTIA, Paris, 135 Pages.
22. **GUILLON Bernard (2008)**, méthodes et thématiques pour la gestion des risques. Edition L'Harmattan, paris, 364 Pages.
23. **HAMZAOUI Mohamed (2008)**, Audit : Gestion des risques d'entreprise et Contrôle interne. Edition Pearson Education France, 243 pages
24. **IFACI (1990)**, Les principes de sécurité informatique: Guide d'audit, Edition CLET, Paris, 229 Pages.
25. **IFACI, PRICEWATERHOUSECOOPERS et Al. (1994)**, La nouvelle pratique du contrôle interne, Les Editions d'Organisation, Paris,
26. **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.
27. **JIMENEZ Christian (2008)**, Risques opérationnels, Edition Revue Banque, Paris, 270 Pages.
28. **LAFITTE Michel (2003)**, Sécurité des systèmes d'information et maîtrise des risques. Revue banque Edition, 127 pages
29. **LAUDON C. Kenneth LAUDON P Jane et GRINGRAS Lin (2000)**, Les systèmes d'information de gestion, Pearson Education/Village Mondial, Paris, 784 Pages.
30. **LY Henry (2005)**, L'audit technique informatique, Edition HERMES, Paris, 230 pages.
31. **MADERS Henri Pierre & MASSELIN Jean Luc (2006)**, Contrôle interne des risques : Cibler, Evaluer, Organiser, Piloter, Maîtriser. Edition d'organisation, 261 pages
32. **MENTHONNEX Jean (1995)**, Sécurité et qualité informatique. Nouvelles orientations, Presses Polytechniques et Universitaires Romandes, Lausanne, 422 Page

33. **MOISAND Dominique et GARNIER DE LABAREYRE, Fabrice (2009)**, Cobit: Pour une meilleure gouvernance des systèmes d-information, Edition EYROLLES, Paris, 258 Pages.
34. **MOREAU Franck (2002)**, Comprendre et gérer les risques, Editions d'Organisation, Paris, 222 Pages.
35. **NICOLET Jean-Louis, (2010)**, Risques et complexité. Edition L'Harmattan, Paris, 422 Pages.
36. **POULIOT Daniel & BILODEAU Yves (2002)**, Mesurer les risques en vue de les contrôler et de les gérer. Revue Audit, N°160, pages 35-37
37. **PRICEWATERHOUSECOOPERS (2009)**, Gestion de la PME: Guide pratique du chef d'entreprise et de son conseil, Editions FRANCIS LEFEBVRE, Paris, LAVALLOIS, 777 Pages.
38. **REIX Robert (2005)**, Systèmes d'information et management des organisations, 5ème édition, LIBRAIRIE VUIBERT, Paris, 486 Pages.
39. **RENARD Jacques (2010)**, Théorie et pratique de l'audit interne, 7ème édition, Les Editions d'Organisation, Paris, 486 Pages.
40. **ROUFF Jean-Loup (2008)**, Renforcer la gouvernance et la gestion des risques, COSO II REPORT Revue Audit, N°178, page 48.
41. **ROYER Jean Marc (2004)**, Sécuriser l'informatique de l'entreprise: Enjeux, menace, prévention et parade, Edition ENI, paris, 422 Pages.
42. **SHICK Pierre & LEMANT Olivier (2002)**, Guide de self-audit, Edition d'Organisation, Paris, 218 Pages.
43. **SHICK Pierre (2007)**, Mémento de l'audit interne. Méthodes de conduite d'une mission. DUNOD, 2ème édition, Paris, 217 Pages.
44. **SHICK Pierre et Al. (2010)**, Audit interne et référentiels des risques, DUNOD, Paris, 340 Pages.