



**Centre Africain d'Etudes Supérieures en Gestion**

**CESAG-EXECUTIVE  
EDUCATION**

**MBA en Audit et Contrôle de  
Gestion  
(MBA-ACG)**

**Promotion 28  
(2016-2017)**

**Mémoire de fin d'Etudes**

**THEME :**

**DIAGNOSTIC DE LA DEMARCHE  
D'ELABORATION DE CARTOGRAPHIES DES  
RISQUES AU CABINET MARISYS SENEGAL**

**Présenté par :**

**AKAMBI Cédric**

**Dirigé par :**

**Mme KANE Mame Rouba**

Enseignante – Chercheur au Centre Africain  
d'Etudes Supérieures en Gestion (CESAG)

**Avril 2018**

## DEDICACE

Nous dédions ce travail à nos défunts parents, à tous nos frères et sœurs pour leur soutien.

CESAG - BIBLIOTHEQUE

## REMERCIEMENTS

Nous témoignons nos profondes gratitude et remerciements les plus sincères à DIEU tout puissant lui dont la volonté et la grâce nous a permis d'aboutir à ce travail.

Nous adressons également nos remerciements :

- À Madame KANE Mame Rouba, enseignante chercheur au Centre Africain d'Etudes Supérieures en Gestion (CESAG) pour l'encadrement et les conseils prodigués tout au long de la rédaction de notre mémoire ;
- À Monsieur TINE Mor Badiane, associé gérant du cabinet MARISYS Sénégal pour nous avoir accepté au sein de sa structure et pour ses conseils ;
- À Monsieur SERE Souleymane pour ses conseils servant à la rédaction de notre mémoire ;
- À notre Chef de département Dr TIOTE Lassana pour sa disponibilité et ses conseils ;
- À l'ensemble du personnel du cabinet MARISYS Sénégal ;
- À Notre grande sœur AKAMBY Ange Elodie pour son soutien moral et financier ;
- À tous nos frères et sœurs pour leur soutien ;
- À tous ceux, qui de près ou de loin ont contribué à rédaction de ce mémoire.

## LISTE DES SIGLES ET ABREVIATIONS

CI	: Contrôle Interne
COSO	: Committee Of Sponsoring Organizations of the Treadway Commission
DSI	: Direction du Système d'Information
IFACI	: Institut Français de l'Audit et du Contrôle Interne
GSI	: Gouvernance du Système d'Information
MARISYS	: Système Intégré de Maitrise des Risques
PA	: Plan d'Action
PV	: Procès-Verbal
SDI	: Schéma Directeur Informatique
TMA	: Tierce Maintenance Applicative

## LISTE DES TABLEAUX

Tableau 1 : Synthèse des différentes approches méthodologiques d'élaboration de cartographies des risques.....	18
Tableau 2 : Matrice des risques.....	22
Tableau 3 : Représentation des sous processus de la DSI.....	42
Tableau 4 : Risques potentiels identifiés par processus.....	43
Tableau 5 : Risques potentiels retenus pour analyse.....	44
Tableau 6 : Les différents types de risques.....	45
Tableau 7 : Identification des causes et des conséquences probables.....	46
Tableau 8 : Echelle d'évaluation de la probabilité de survenance du risque.....	51
Tableau 9 : Echelle d'évaluation de l'impact de survenance du risque.....	52
Tableau 10 : Evaluation du risque inhérent, identification des bonnes pratiques et des éléments clés du contrôle interne.....	55
Tableau 11 : Echelle de cotation des risques inhérents.....	61
Tableau 12 : Grille d'évaluation de la protection.....	61
Tableau 13 : Grille d'évaluation de la prévention.....	62
Tableau 14 : Mesure ou évaluation des éléments du contrôle interne.....	62
Tableau 15 : Echelle de mesure du risque résiduel.....	63
Tableau 16 : Evaluation du contrôle interne, risque résiduel et recommandations.....	64
Tableau 17 : Proposition du plan d'actions.....	72

## LISTES DES FIGURES

Figure 1: Présentation combinée des démarches Bottom up et Top down .....	16
Figure 2 : Hiérarchisation des risques .....	22
Figure 3 : Matrice SWOT.....	25
Figure 4 : Modèle d'analyse .....	27

CESAG - BIBLIOTHEQUE

## LISTE DES ANNEXES

Annexe 1 : Organigramme du Cabinet MARISYS Sénégal du 12/01/2018 .....	86
Annexe 2 : Matrice MARISYS .....	87

CESAG - BIBLIOTHEQUE

## SOMMAIRE

DEDICACE.....	i
REMERCIEMENTS .....	ii
LISTE DES TABLEAUX.....	iv
LISTES DES FIGURES.....	v
LISTE DES ANNEXES.....	vi
SOMMAIRE .....	vii
INTRODUCTION GENERALE.....	1
PREMIERE PARTIE : CADRE THEORIQUE ET CONCEPTUEL.....	7
CHAPITRE 1 : LE CADRE CONCEPTUEL ET THEORIQUE DE LA CARTOGRAPHIE DES RISQUES.....	9
CHAPITRE 2 : ETAT DE LA LITTERATURE SUR LE DIAGNOSTIC DE LA DEMARCHE D'ELABORATION DE CARTOGRAPHIES DES RISQUES .....	15
CHAPITRE 3 : METHODOLOGIE DE L'ETUDE.....	26
DEUXIEME PARTIE : CADRE PRATIQUE DE L'ETUDE .....	31
CHAPITRE 4 : PRESENTATION DE MARISYS SENEGAL.....	33
CHAPITRE 5 : DESCRIPTION DE LA DEMARCHE D'ELABORATION D'UNE CARTOGRAPHIE DES RISQUES D'UNE DIRECTION DU SYSTEME D'INFORMATION.....	37
CHAPITRE 6 : DIAGNOSTIC DE LA DEMARCHE D'ELABORATION D'UNE CARTOGRAPHIE DES RISQUES.....	76
CONCLUSION GENERALE .....	84
ANNEXES .....	85
BIBLIOGRAPHIE .....	90



## INTRODUCTION GENERALE

CESAG - BIBLIOTHEQUE

Scandales financiers avec les affaires telles que Worldcom, Tyco, Enron, Parmalat, le crédit lyonnais, falsification de documents, ou encore site internet piraté, ne cessent de nous prouver que partout dans le monde les entreprises évoluent dans un environnement de plus en plus incertain. Selon (IFACI et al. 2005), l'incertitude est une donnée intrinsèque à la vie de toute organisation, on remarque immédiatement que les entreprises sont confrontées à des événements qui pourraient être un frein à l'atteinte de leurs objectifs. Dans cette même veine pour le Committee Of Sponsoring Organizations of the Treadway Commission (COSO 2), la possibilité qu'un événement se produise et ait une incidence défavorable sur la réalisation des objectifs est appelé risque. Par ailleurs, le Guide (2009 : 73) « Management du risque – Vocabulaire », la norme ISO 31000 in (IFACI, 2013 : 30) définit plus simplement le risque comme étant l'effet de l'incertitude sur l'atteinte des objectifs. Ainsi, si les risques non maîtrisés peuvent empêcher l'atteinte des objectifs des entreprises, c'est le lieu de se poser la question sur la nécessité d'un management des risques au sein de celles-ci.

Le management des risques se définit comme « un processus mis en œuvre par le conseil d'administration, la direction générale, le management et l'ensemble des collaborateurs de l'organisation. Il est pris en compte dans l'élaboration de la stratégie ainsi que dans toutes les activités de l'organisation. Il est conçu pour identifier les événements potentiels susceptibles d'affecter l'organisation et pour gérer les risques dans les limites de son appétence pour le risque. Il vise à fournir une assurance raisonnable quant à l'atteinte des objectifs de l'organisation » (COSO 2). De cette définition, la nécessité de doter toute entreprise d'outils de gestion de risque devient une obligation bien plus qu'une nécessité car ils permettront à l'entreprise d'avoir une vue sur les risques auxquels elle est confrontée, d'assurer une maîtrise de ces risques en mettant en place des processus efficaces de protection ou de prévention, et enfin d'assurer une gestion efficace et efficiente des ressources de l'entreprise dans le but d'atteindre ses objectifs.

La gestion des risques peut se faire à l'aide des outils comme la cartographie des risques. Selon l'IFACI (2013 :10) « la cartographie des risques est une démarche dynamique d'identification et d'évaluation des risques qui permet d'en donner une représentation synthétique et visuelle. Elle constitue ainsi un outil de mise en évidence des risques à couvrir en priorité ». En effet, la cartographie des risques permet d'identifier les risques majeurs d'une entreprise, de les présenter de façon hiérarchisée de sorte à avoir une vision sur les priorités aux niveaux des risques et cela en se basant sur la probabilité de survenance, le degré de l'impact et la vulnérabilité de l'entreprise. Par ailleurs, l'établissement d'une cartographie

des risques peut être motivé par des objectifs de différentes natures aussi importants les uns que les autres. Parmi lesquels nous pouvons citer :

- la mise en place d'un contrôle interne ;
- la mise en place d'un processus efficace de gestion de risque ;
- l'assistance à la direction dans l'élaboration de son plan stratégique ;
- le soutien de l'audit interne lui permettant d'avoir une vision sur les processus ayant un niveau de risques élevé ;
- l'élaboration d'un plan d'audit basé sur les risques.

Malgré l'importance de cet outil de gestion des risques, on constate que certaines entreprises n'en disposent pas. Cela peut s'expliquer par :

- une mise en place difficile de la cartographie des risques ;
- l'inefficacité de certaines démarches d'élaboration de cartographies des risques ;
- le choix difficile d'une démarche à adopter pour l'élaboration d'une cartographie des risques ;
- la complexité de certaines démarches d'élaboration de cartographies des risques.

De ce qui précède, il découle que ces entreprises vivant dans un environnement en pleine évolution seront confrontées à plusieurs problèmes liés à leur gestion vu la méconnaissance des obstacles qui freinent l'atteinte de leurs objectifs et leur exposition à plusieurs risques à savoir :

- risque financier ;
- risque opérationnel ;
- risque informatique ;
- risque ressource humaine ;
- risque économique ;
- risque stratégique ;
- risque de fraude, corruption, détournement ;
- risque juridique ;
- risque réputation ;
- risque d'intégrité ;
- risque de défaillance ;
- risque d'approvisionnement ;

- risque environnemental ;
- risque démographique.

Pour pallier les problèmes, plusieurs solutions s'offrent aux entreprises à savoir faire appel à des prestataires spécialisés tels que les cabinets d'expertise comptable ou les cabinets de conseils disposant des méthodes minutieuses pour l'élaboration d'une cartographie des risques parmi lesquels on peut citer le cabinet MARISYS SENEGAL, expert dans le domaine de la gestion des risques. Nous pouvons aussi retenir entre autres solutions :

- la recherche d'une démarche efficace pour l'élaboration de cartographies des risques ;
- la recherche d'une démarche peu complexe pour l'élaboration de cartographies des risques ;
- la recherche de meilleure pratique en matière de gestion de risque.

La solution que nous retenons et qui nous paraît plus adéquate est la recherche d'une démarche efficace pour l'élaboration de cartographies des risques.

Du fait que nous soyons en stage dans le cabinet MARISYS SENEGAL, et vue notre quête de démarche efficace pour l'élaboration de cartographies des risques, nous comptons procéder à un diagnostic de la démarche de ce cabinet pour l'élaboration de cet outil. Ce qui nous paraît plus adéquate dans la recherche d'une démarche efficace. En effet le Cabinet MARISYS SENEGAL, notre Cabinet d'accueil, détient à son actif plusieurs missions de formation et de conception de cartographies des risques.

Au regard de la solution retenue, la principale question de recherche à laquelle nous essayerons d'apporter des réponses est la suivante : « la démarche d'élaboration de cartographies des risques adoptée par le cabinet MARISYS est-elle appropriée ? »

De cette question principale, ressortent les questions spécifiques suivantes :

- comment est la démarche du cabinet MARISYS pour l'élaboration d'une cartographie des risques ?
- quelles sont les différentes phases de la démarche du cabinet MARISYS pour l'élaboration d'une cartographie des risques ?
- quelles sont les forces de la démarche de MARISYS pour l'élaboration d'une cartographie ?

- quelles sont les faiblesses de la démarche de MARISYS pour l'élaboration d'une cartographie ?
- quelles sont les recommandations à faire pour améliorer cette démarche ?

La recherche de réponses à ces différentes questions justifie le choix de notre thème : « Diagnostic de la démarche d'élaboration de cartographies des risques au cabinet MARISYS SENEGAL. »

L'objectif général de notre travail sera de comprendre et d'apprécier la démarche d'élaboration de cartographies des risques du cabinet MARISYS Sénégal.

Il s'agira plus spécifiquement :

- de comprendre la démarche d'élaboration de cartographies des risques du cabinet MARISYS Sénégal ;
- de faire ressortir les forces de la dit démarche ;
- de faire ressortir ces faiblesses ;
- de faire des recommandations dans le cadre d'une amélioration de cette démarche.

De cette étude découlera directement des intérêts situés à trois niveaux :

- Pour le cabinet MARISYS, ce travail lui permettra de prendre conscience des faiblesses de sa démarche et d'apporter des corrections voire, prendre des dispositions pour une amélioration pour satisfaire au mieux sa clientèle ainsi qu'accroître le nombre de ses interventions auprès des entreprises.
- Pour le lecteur ce travail, il lui permettra de comprendre la démarche du cabinet MARISYS dans l'élaboration d'une cartographie de risque.
- Pour nous même, ce travail sera un approfondissement sur les démarches d'élaboration d'une cartographie des risques et sur comment faire un diagnostic. Il nous permettra aussi d'être mieux outillés pour la gestion des risques en entreprises d'où avoir une base pour mieux embrasser le métier de risk manager.

Ce mémoire s'articulera autour de deux parties :

- une première partie consacrée au cadre théorique de notre recherche et de la méthodologie. Elle comprend trois chapitres : le premier mettant en exergue des concepts fondamentaux du management des risques, le deuxième traitant des

différentes démarches d'élaboration de cartographies des risques, de la démarche et outils de diagnostic d'une démarche de cartographie des risques et le troisième abordant la méthodologie de recherche de notre étude.

- et une deuxième partie consacrée au cadre pratique du diagnostic de la démarche d'élaboration de cartographies des risques au cabinet MARISYS. Elle comprend également trois chapitres : le premier permettant de mieux connaître le cabinet MARISYS, le deuxième décrivant la démarche d'élaboration d'une cartographie des risques du cabinet MARISYS par son application à un cas X parmi les clients du cabinet dont nous nous gardons de taire le nom afin de préserver l'anonymat, et le troisième analysant les forces et faiblesses de cette démarche afin de faire des recommandations dans le but de contribuer à son amélioration.

CESAG - BIBLIOTHEQUE

**PREMIERE PARTIE : CADRE THEORIQUE ET  
CONCEPTUEL**

## INTRODUCTION DE LA PREMIERE PARTIE

La gestion du risque est aujourd'hui l'un des défis auxquels les entreprises doivent faire face dans un environnement de plus en plus à risque.

Pour assurer une gestion optimale des risques et atteindre leurs objectifs, les entreprises doivent donc mettre en place des outils qui leur permettront de maîtriser les risques auxquels elles sont confrontées dans leur quotidien.

Dans le cadre de notre première partie nous nous intéresserons aux théories et démarches d'élaboration d'une cartographie des risques.

Ainsi dans le premier chapitre il sera question pour nous d'aborder le cadre conceptuel et théorique de la cartographie des risques, dans le deuxième chapitre nous ferons un état de la littérature sur les démarches, diagnostic d'élaboration de cartographies des risques et pour terminer avec le troisième chapitre dans lequel il sera question pour nous d'aborder notre méthodologie de l'étude.



# CHAPITRE 1 : LE CADRE CONCEPTUEL ET THEORIQUE DE LA CARTOGRAPHIE DES RISQUES

Pour mieux cerner le concept de cartographies des risques nous allons présenter les notions générales concernant la cartographie des risques et les éléments qui entourent ces notions.

## 1.1. Notion du risque

Toute entreprise étant confrontée à un certain nombre de risques, il faudrait songer comme nous l'avons souligné dans l'introduction générale à cartographier ces risques, cependant pour cartographier il faudrait comprendre la notion du risque.

### 1.1.1. Définition du risque

Selon Darsa & Dufour (2014 :14) « Le risque est fréquemment défini comme un événement imprévu ou un ensemble de conditions réduisant de manière importante l'habileté des gestionnaires dans la conduite de la stratégie d'affaires envisagée. Cette approche rassurante pour certains (les managers) ne l'est pas forcément pour tous. »

Cette définition montre que le risque est tout ce qui pourrait réduire d'une manière importante la capacité des managers dans la conduite de la stratégie.

Bernard & al (2006 :68) dans cette même veine définissent le risque comme « Un événement éventuel dont la survenue réelle est susceptible de provoquer un dommage non négligeable à l'organisation ». De cette définition, il ressort que le risque est un événement éventuel dont la conséquence serait d'un grand dommage pour l'entreprise.

Complétons ces définitions par celle de Gaultier-Gaillard & Louisot (2014 :31) qui disent ceux-ci « Un risque est événement ou une série d'événements dont la réalisation pourrait mettre en péril la réalisation des objectifs. ». Cette définition nous fait comprendre que le risque est tout événement qui pourrait être une entrave à l'atteinte ou à la réalisation des objectifs.

De tout ce qui précède, on peut dire que le risque est la survenance d'un événement indésirable qui pourrait causer un dommage.

### **1.1.2. Les types de risques**

Selon IFACI & PricewaterhouseCoopers (2015 : 71) « toute entité est confrontée à une diversité de risques, provenant de sources externes et internes » ici on remarque que peu importe la typologie du risque il sera cependant externe ou interne.

Sean & al (2006 :75-76), suggèrent de regrouper tous les risques auxquels peut faire face une entreprise en quatre catégories distinctes :

- Les risques stratégiques ;
- Les risques financiers ;
- Les risques opérationnels ;
- Les risques projets ;

#### **1.1.2.1. Les risques stratégiques**

Selon Maders & Masselin (2014 : 16), le risque stratégique « Appelé aussi « risque de politique générale » ou « de management », il correspond au risque lié à une absence de stratégie ou à une stratégie déficiente sur un ou plusieurs métiers de l'entreprise ».

Une autre définition est celle de Pierandrei (2015 : 61) pour qui « Le risque stratégique se définit comme le risque lié aux choix stratégiques d'une entreprise dans le but de s'adapter à son environnement concurrentiel. ».

Nous terminerons avec cette définition de Sean & Al (2006 :75) pour qui « les risques stratégiques menacent la survie de la firme ou sa capacité à maintenir une activité rentable et de création de valeur pour l'actionnaire ; ils peuvent faire suite à des changements dans l'environnement du marché, à une catastrophe naturelle ou encore résulter de l'activité humaine. ».

#### **1.1.2.2. Les risques financiers**

Selon Sean & Al (2006 : 75-76) « les risques financiers menacent la solvabilité, la rentabilité et la trésorerie de l'entreprise, et peuvent découler des mouvements de prix du marché (variation des cours des devises, des taux d'intérêts, des primes d'assurances, des cours des actions, des opérations de couverture, des options et autres produits dérivés), de la faillite d'un partenaire, d'un retard de règlements ou d'événements similaires. ».

#### **1.1.2.3. Les risques opérationnels**

Pour Dufour & Teneau (2013 :189) « les risques opérationnels peuvent être définis comme des risques de pertes provenant des erreurs du personnel au sens large, des systèmes ou

processus, ou des événements externes, tels que les risques de détérioration affectant les outils de production, les risques technologiques, les risques climatiques, ou encore les risques environnementaux. ».

Complétons cette définition par celle de Pierandrei, (2015 : 61) « Le risque opérationnel peut être défini comme le risque qui ne dépend pas de la façon de financer une entreprise, mais plutôt de la façon dont elle opère son métier. »

#### **1.1.2.4. Les risques projets**

Le PMBOK in (Dufour & Teneau, 2013 :179) définit le risque projet comme étant un événement ou une situation dont la concrétisation, incertaine, aurait un impact positif ou négatif sur les objectifs du projet.

Pour Sean & Al (2006 : 76), « les risques projets surviennent dans le cadre de programmes ou de projets distincts et comprennent généralement des risques impliquant des problèmes technologiques, des comportements humains, des processus peu familiers et des menaces externes. »

## **1.2. Notion de la cartographie des risques**

Pour cartographier, il faudrait comprendre la notion de cartographie des risques.

### **1.2.1. Définition de la cartographie des risques**

Selon Jean-Paul Louisot, (2014 : 51) « il est devenu usuel dans la profession d'appeler « carte des risques », à un instant donné, un tableau à double entrée : sur un axe, les probabilités (fréquence ou vraisemblance) et sur l'autre, l'impact. C'est de là que vient le nom de cartographie des risques, ou de cartographier pour nommer le diagnostic des risques. ».

Pour Darsa (2015 :189) « Cartographier les risques de l'entreprise consiste à représenter visuellement, ou plutôt graphiquement, les zones de risque en présence. La démarche de cartographie a donc pour objet de simplifier la représentation des enjeux prioritaires à traiter au titre de la gestion des risques. Cette dimension visuelle est importante car elle permet une appropriation de l'enjeu plus factuelle, donc plus accessible, plus compréhensible. Très souvent, une carte, un dessin, seront plus parlants qu'un tableau de chiffres, surtout lorsque ce dernier consolide 4 critères et 365 risques individuels ! ». De cette définition il ressort que la cartographie est la vision nette en image des zones à niveau de risques important d'une organisation dans le but de les traiter dans le management des risques.

Terminons cette définition par celle de Moreau & al. (2002 :123) « La cartographie des risques est un outil de management que peut élaborer une entreprise afin d'obtenir une vision globale des risques qu'elle encourt, notamment en matière informatique. »

### 1.2.2. Les objectifs de la cartographie des risques

Selon Renard (2017 :149), la cartographie est un véritable inventaire des risques de l'organisation, qui permet d'atteindre trois objectifs :

- inventier, évaluer et classer les risques de l'organisation ;
- informer les responsables afin que chacun soit en mesure d'y adapter le management de ses activités ;
- permettre à la direction générale, et avec l'assistance du risk manager, d'élaborer une politique de risque qui va s'imposer à tous :
  - aux responsables opérationnels dans la mise en place de leur système de contrôle interne ;
  - aux auditeurs internes pour élaborer leur plan d'audit, c'est-à-dire fixer les priorités.

Selon Bernard & al (2013 :84) composante essentielle du processus de gestion des processus, la cartographie des risques vise à relier à chaque niveau opérationnel et décisionnel, pour chaque entité et pour chaque processus clé :

- une série de risques identifiés ;
- leurs causes ;
- leurs impacts ;
- les leviers d'actions possibles ;
- les retours d'expérience sur les sinistres antérieurs

### 1.2.3. Les acteurs de la cartographie des risques

Selon Renard (2017 : 149) il y'a principalement trois acteurs de la cartographie des risques :

- le risk manager : son rôle est défini par la norme ISO 31000. On peut le résumer en disant qu'il identifie les risques, en dessine la cartographie, les mesure et, à partir de là, propose la politique qui sera appliquée dans le double domaine de la prévention et de la protection ;
- le manager opérationnel applique cette politique et met en place les moyens pour maîtriser les risques inacceptables et limiter les risques acceptables (contrôle interne) ;

- l'auditeur interne apprécie la qualité de la cartographie et des moyens mis en place ; il en détecte les lacunes et les insuffisances et formule des recommandations pour y mettre fin. Mais il n'est pas concerné par l'élaboration et la mise en place d'une gestion globale des risques.

#### **1.2.4. Les motivations d'élaboration d'une cartographie**

Plusieurs raisons peuvent motiver les entreprises à élaborer une cartographie à savoir :

- le souci d'avoir une vision d'ensemble, exhaustive et précise, de leur exposition aux turbulences de toutes natures, tant internes qu'externes ;
- dans la recherche des dispositifs adéquats à mettre en place pour maîtriser ces risques ;
- en termes de projet : la cartographie permet au chef de projet de synthétiser sa réflexion sur les facteurs de risque du projet et de prendre les mesures préventives permettant d'éviter l'apparition de ces risques ainsi que les mesures curatives permettant d'en limiter les effets. Schick (2010 : 64), Maders & al (2014 :19)

#### **1.2.5. Les types de cartographie des risques**

L'une des premières questions auxquelles l'on doit répondre avant l'élaboration d'une cartographie des risques est de savoir le type de cartographie que l'on souhaite élaborer.

##### **1.2.5.1. La cartographie globale**

Jean Le Ray (2015 : 288) « La cartographie globale des risques est une vision de la vulnérabilité de l'organisme à un instant T. Elle devra être revue régulièrement, une fois par an dans sa globalité et plus fréquemment pour les domaines de risques qui, de par leur variabilité, font l'objet d'une surveillance accrue. ».

##### **1.2.5.2. La cartographie thématique**

La cartographie thématique permet de recenser et d'hierarchiser les risques liés à un domaine ou un thème précis. Son principal intérêt est de pouvoir réunir et comparer sur un même thème :

- soit différentes organisations pour un même thème de risques ;
- soit différents domaines de risques liés au même thème étudié pour une même organisation (De Mareschal 2006 ; 7)

#### **1.2.6. Les facteurs clés de succès d'une cartographie des risques**

Plusieurs facteurs peuvent contribuer à la réussite d'une cartographie des risques :

➤ **Volonté forte des dirigeants**

Cette volonté doit se trouver à deux niveaux :

- Le Conseil d'Administration ou Conseil de Surveillance tout d'abord, dont le Président, il faut le rappeler, se doit de produire le « Rapport du Président » sur les procédures de contrôle interne. Or l'identification et l'évaluation des risques est à la base d'un bon dispositif de contrôle interne. Lorsqu'il existe, le Comité d'Audit est le lieu privilégié où doit se manifester cette volonté.
- La Direction Générale, qui doit donner l'impulsion à l'ensemble du dossier, mais surtout créer les conditions et mettre en place les moyens de réaliser cette cartographie des risques, ce qui passe inévitablement par l'allocation de ressources dédiées. Plus largement, le Comité de Direction doit être complètement partie prenante, ne serait-ce que parce que chaque Directeur, qu'il soit opérationnel ou fonctionnel, doit initier cette démarche dans sa propre Direction.

➤ **Passage par la cartographie des processus**

Il y a de multiples raisons d'élaborer une cartographie des processus dans une entreprise : simple modélisation des process, migration d'un système d'information vers un autre, harmonisation des process après fusion d'entreprise. Mais il en est au moins une qui la rend indispensable : l'élaboration de la cartographie des risques. D'une façon générale, nous retrouvons trois grandes catégories de processus :

- les processus métiers, ou processus opérationnels, ou processus de réalisation : vente, souscription, production, sinistre ;
- les processus managériaux ou de pilotage : stratégie, plans d'actions, budget ;
- les processus supports : ressources humaines, finances, comptabilité, informatique, logistique IFACI (2006 :13)

## **Conclusion**

Ce chapitre nous a permis de mettre en exergue les différentes notions sur le risque et la cartographie des risques, dans le chapitre suivant nous aborderons l'état de littérature sur les démarches de diagnostic et d'élaboration de cartographies des risques.

## CHAPITRE 2 : ETAT DE LA LITTERATURE SUR LE DIAGNOSTIC DE LA DEMARCHE D'ELABORATION DE CARTOGRAPHIES DES RISQUES

Pour avoir une idée sur le diagnostic de la démarche d'élaboration de la cartographie des risques, nous allons présenter les différentes approches d'élaboration de cartographies des risques et montrer comment faire un diagnostic. Le terme approche sera utilisé dans cette partie car la plupart des auteurs l'utilise pour faire allusion au terme démarche. Ainsi dans notre étude nous ne ferons pas de distinction entre approche et démarche.

### 2.1. Les différentes approches de cartographie des risques

L'approche de la cartographie des risques diffèrent d'un auteur à un autre. Ainsi, par synthèse, six (6) différentes approches se présentent :

- l'approche Top down ;
- l'approche Bottom up;
- l'approche Combinée ;
- le Benchmarking ;
- l'auto-évaluation ;
- l'approche par analyse.

#### 2.1.1. L'approche Top down

Selon Cordel & Al (2013 : 131), « Elle consiste à collecter en premier lieu la vision des équipes dirigeantes et des organes de gouvernance, puis à la partager à tous les niveaux de l'organisation. ». L'avantage de cette approche est qu'elle mettra clairement en exergue la volonté de la direction générale de donner une impulsion dans la mise en évidence au niveau global et mettra l'accent sur la nécessité d'une adhésion du management décisionnel (Dufour & Al, 2013 : 33).

#### 2.1.2. L'approche Bottom up

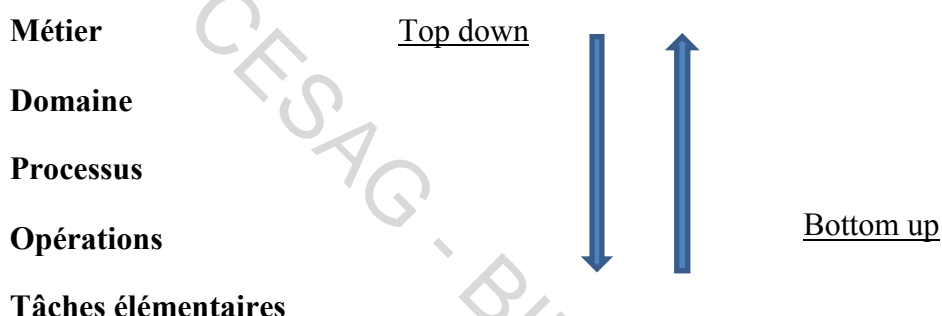
L'approche bottom up (de bas en haut) est l'approche qui donne la priorité aux personnes concernées par la gestion du risque au quotidien : les opérationnels (Cordel & Al, 2013 : 131). Elle permettra selon (Dufour & Al, 2013 : 33-34), « de mieux apprécier des risques opérationnels a priori de faible impact, mais dont le cumul, l'agrégation, peut avoir un impact non négligeable pour l'entreprise. Une telle approche permet encore de mieux détecter les

risques orphelins (n'ayant pas de propriétaires de risques à proprement parler, il s'agira alors de risques transverses entre plusieurs fonctions), d'obtenir davantage d'informations sur chaque risque afin d'y allouer les ressources de la manière la plus optimale qui soit. »

### 2.1.3. L'approche combinée

Comme son nom l'indique, cette approche permet la combinaison des deux approches citées précédemment. C'est-à-dire l'approche Top up et l'approche Bottom down. Selon l'approche combinée, c'est l'identification des risques faite parallèlement par la hiérarchie et les opérationnels qui permet à l'entreprise d'avoir une base assez complète de ses risques.

Figure 1: Présentation combinée des démarches Bottom up et Top down



Source : IFACI (2006 : 14)

### 2.1.4. L'approche par le benchmarking

Selon Jiminez & Al (2008 :103), cette approche consiste à étudier et analyser les meilleures pratiques d'établissement d'une cartographie des risques des entreprises exerçant les métiers similaires et ayant les mêmes processus afin de s'en inspirer et d'en retirer le meilleur. Autrement dit, c'est une méthode qui consiste à progresser en allant chercher ce qu'il y a de mieux chez le voisin (Renard, 2003 : 225).

### 2.1.5. L'approche par l'autoévaluation

Elle permet d'éviter une fonction d'audit interne lourde et souvent très mal perçue par les opérationnels (Colatrella, 2006 : 7). Dans l'autoévaluation, la responsabilité du contrôle interne est confiée par le management aux opérationnels. Ainsi, elle permet aux opérationnels de s'approprier la démarche du contrôle interne.



### **2.1.6. L'approche par analyse et synthèse des rationnelles des risques**

Cette approche, selon Ernst & Young (2004 : 4), consiste à faire une comparaison entre l'existant, les données chiffrées et un référentiel de bonnes pratiques recueillies sous forme de Benchmarking.

## **2.2. Les différentes étapes d'élaboration d'une cartographie des risques**

N'ayant pas une démarche standard d'élaboration d'une cartographie des risques, la présente partie sera faite sur la base d'une synthèse des différents auteurs. Cette synthèse a été faite dans le tableau ci-dessous :

CESAG - BIBLIOTHEQUE

Tableau 1 : Synthèse des différentes approches méthodologiques d'élaboration de cartographies des risques

PHASES/AUTEURS	ETAPES	Jimenez & Al (2008 : 65)	Renard & Al (2006 : 141, 176)	Curaba & Al (2009 :160)	Moreau & Al (2002 :163)	IFACI (2006 :19)
Préparation	Prise de connaissance générale de l'entreprise	X	X			
	Prise de connaissance de l'activité concernée	X	X			
	Analyse de l'activité concernée	X	X	X	X	X
	Elaboration d'une nomenclature des risques	X	X			
Planification	Identification et analyse des risques	X	X	X	X	X
	Evaluation des risques	X	X	X	X	X
	Appréciation globale de chaque risque de l'activité		X			
	Hierarchisation des risques	X	X	X		X
	Matrice des risques	X	X	X	X	X
Action	Définition et mise en place du plan d'actions	X		X	X	X
Reporting	Reporting sur les risques résiduels et le plan d'actions	X				
Suivi évaluation	Vérification de l'efficacité du plan d'action	X		X	X	
Actualisation	Amélioration et mise à jour de la démarche	X		X		X

Source : les auteurs cités dans le tableau de synthèse

### 2.3. Analyse du tableau de synthèse

Au regard du précédent tableau, nous déduisons six (6) phases d'élaboration d'une cartographie des risques, à savoir :

- la phase de préparation ;
- la phase de planification ;
- la phase d'action ;
- la phase de reporting ;
- la phase de suivi ;
- la phase d'actualisation.

Au regard du tableau, force est de constater que les étapes d'élaboration de la cartographie des risques proposés par Jimenez & Al couvrent presque toutes les étapes.

#### 2.3.1. Phase de préparation

Du fait des choix stratégiques, du mode d'organisation, du système d'information et des activités, il est évident que chaque entreprise a ses propres spécificités. L'intérêt de cette phase s'explique donc par le fait qu'elle doit permettre de comprendre l'organisation de la structure et d'établir la nomenclature des risques (JIMENEZ & Al, 2008 :64).

#### 2.3.2. Phase de planification

La planification pourrait être définie comme étant la programmation d'actions et d'opérations à mener pour atteindre un résultat. Elle est la phase la plus importante du processus et représente la mise en œuvre de la démarche. Elle se déroule en un certain nombre d'étapes, à savoir :

- l'identification et l'analyse des risques ;
- l'évaluation des risques ;
- l'appréciation globale de chaque risque de l'activité ;
- La hiérarchisation des risques ;
- la matrice des risques.

##### 2.3.2.1. Identification et analyse des risques

Le processus d'identification et d'analyse du risque est un élément clé d'un système de contrôle interne efficace (Bertin, 2007 : 71). L'Organisation Internationale de Normalisation (ISO) a défini l'identification des risques comme étant le processus de recherche, de reconnaissance et d'enregistrement des risques. Cette identification des risques a pour objet

d'identifier les raisons pour lesquelles les objectifs du système ou de l'organisation pourraient ne pas être atteints (Cordel & Al, 2013 : 130). L'une des principales difficultés du risk management étant l'identification des risques d'une entreprise de façon objective et rationnelle, il devient ainsi indispensable d'aboutir à la réalisation d'une cartographie des risques qui fait ressortir les méta-risques émergents (Kerebel, 2009 : 19). L'identification des risques passe par plusieurs techniques parmi lesquelles nous retenons :

- l'identification basée sur les check-lists : cette approche consiste à lister un certain nombre de risques éventuels que l'entreprise est supposée encourir et plus tard se poser la question de leurs existences (Curaba & Al, 2009 : 78) ;
- l'identification basée sur l'atteinte des objectifs : elle consiste à analyser les processus et activités de l'entité et de rechercher ensuite les dysfonctionnements qui pourraient impacter les objectifs ou les résultats attendus (IFACI, 2006 : 19) ;
- l'identification par les tâches élémentaires : cette approche est bien connue des auditeurs car ils l'utilisent lors de la construction du questionnaire du contrôle interne (Renard, 2006 : 176). Elle permet de répondre à la question suivante : que se passerait-il si une tâche est mal faite ou pas du tout faite ?
- l'identification par l'analyse historique : elle consiste à remonter sur les risques qui ont menacé l'entreprise dans le passé et d'en tenir compte lors de la mise à jour ou de la conception de la carte des risques (Mcnamee, 1998 :13) ;
- l'identification basée sur les scénarios : cette approche consiste à faire recours à des experts de chaque ligne métier et de spécialistes de la gestion des risques (Nicolet & Al, 2005 :51).

#### **2.3.2.2. Evaluation des risques**

L'évaluation des risques permet d'évaluer autant que possible, la probabilité de survenance de chaque risque identifié. Pour ce fait, trois (3) facteurs doivent être combiné :

- la probabilité d'apparition ;
- la gravité en cas de survenance ;
- la durée pendant laquelle les conséquences de l'évènement ont un impact ;

(Maders & Al, 2009 :49).

Cette phase est centrale dans l'élaboration d'une cartographie des risques. Elle s'appuie sur un certain nombre de méthodes à savoir :

- la méthode quantitative : elle consiste à évaluer le risque caractérisant un événement redouté selon sa probabilité et la mesure de sa gravité (Desroches & Al, 2003 : 59),
- la méthode qualitative : moins fiable que la méthode quantitative, la méthode qualitative est utilisée lorsque les risques n'offrent pas de possibilité de quantification ou lorsqu'il n'existe pas suffisamment de données fiables donnant droit à une évaluation qualitative (IFACI, 2006 : 206).

### **2.3.2.3. L'appréciation globale de chaque risque de l'activité**

Au cours des deux (2) méthodes d'évaluation, les appréciations des risques sont laissées à la charge des opérationnels « qui en appréhendent plus aisément les impacts » et des acteurs de la cartographie pour approuver les hypothèses retenues en termes d'impact et de fréquence (IFACI, 2006 : 24). Ces différents acteurs « n'ont pas intérêt à rentrer dans les détails des savants calculs » (Renard & Al, 2006 : 218). Ils peuvent utiliser des échelles d'appréciation telle que celles prônée par Maders & Al (2014 : 67) contenant des cotations de 1 à 5 que voici:

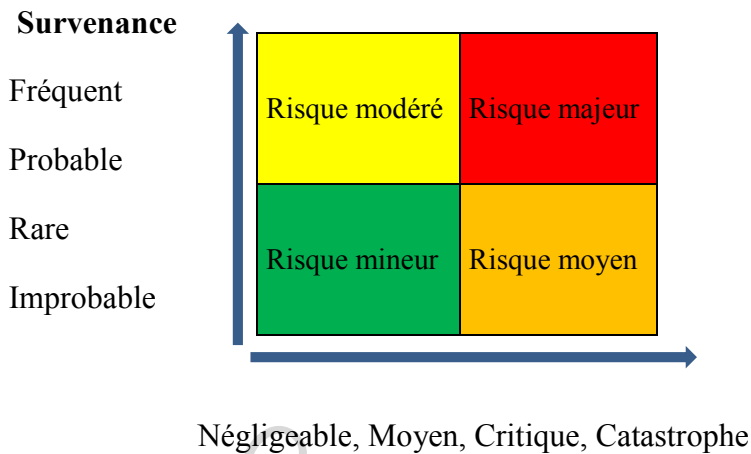
- enjeu financier : de « 5 » = enjeu financier très fort à « 1 » = enjeu financier très faible;
- niveau de vulnérabilité : de « 5 » = vulnérabilité très importante à « 1 » = vulnérabilité très faible ;
- qualité du dispositif de contrôle interne en place : de « 5 » = très mauvais dispositif à « 1 » = très bon dispositif.

### **2.3.2.4. La hiérarchisation des risques**

Selon Curaba & Al (2009 : 24), pour faciliter leur gérance, les risques identifiés et évalués doivent être hiérarchisés. La hiérarchisation des risques s'effectuera suivant la valeur des paramètres de l'évaluation (Jokung, 2008 : 71-72). Trois paramètres vont être présentés :

- survenance et gravité élevées : le risque est dit majeur, il remet en cause les objectifs de l'organisation ;
- survenance et gravité faibles : le risque est qualifié de mineur, il ne remet pas en cause les objectifs de l'organisation ;
- les deux paramètres ne sont pas simultanément faibles ou simultanément élevés, le risque est qualifié d'intermédiaire. Il peut remettre en cause les objectifs de l'entreprise. Au sein des risques intermédiaires, on distingue des risques de gravité élevée et des risques moyens.

Figure 2 : Hiérarchisation des risques



Source : Adaptation de Jokung (2008 : 72)

### 2.3.2.5. La matrice des risques

La matrice des risques est définie comme une représentation graphique de la probabilité d'occurrence et de la gravité de l'impact d'un ou plusieurs risques. Les risques sont donc représentés de sorte à identifier les risques les plus significatifs et les moins significatifs (IFACI, 2006 :221).

Tableau 2 : Matrice des risques

	Fréquence faible	Fréquence élevée
Gravité relative	Risques mineurs (1)	Risques opérationnels (3)
Gravité aigüe	Risques catastrophiques (2)	Evitement (4)

Source : Hassid (2011 : 68)

Selon Hassid (2011 : 68), « la règle générale est qu'une entreprise doit focaliser son attention sur les risques des catégories 2 et 3. Les gestionnaires s'efforcent de réduire les risques de catégories 2 (par la prévention, la protection et autres modes de contrôle). L'évitement s'applique surtout à la catégorie. Les risques de catégorie 3 sont de bons candidats la mutualisation, soit direct de pools ou de mutuelles, soit indirecte par transfert à un spécialiste, en particulier par l'achat de couvertures d'assurances. »

### 2.3.3. La phase d'action

Le but du plan d'action est de pouvoir agir sur les différents éléments identifiés et quantifiés afin de modifier le profil des risques de la société tout au moins sa sensibilité en cas de survenance d'événements non souhaités (Jimenez & Al, 2008 : 127). Pour cela, il convient de

tenir compte de « l'appétence » de l'entreprise pour le risque, autrement dit le niveau de risque que l'entreprise est prête à tolérer et assumer pour atteindre ses objectifs et délimiter ainsi le risque cible, zone de risques jugée acceptable par les dirigeants (KPMG, 2010 :7). Selon Curaba & Al (2009 : 150), le plan d'action doit être structuré en deux parties distinctes. D'une part, le référencement qui permet de comprendre l'origine et le contenu de l'action et d'autre part, la partie pilotage de l'action qui permet d'identifier « qui fait quoi ? » et « quel suivi ».

#### **2.3.4. La phase de reporting**

Selon Masselin et Maders (2014 : 207), « le reporting correspond à un système d'échange d'information structuré entre un acteur du dispositif de contrôle interne et un superviseur. Le plus souvent, le reporting est hiérarchique car le pilotage de l'activité de l'acteur est réalisé par son manager. ». Le reporting sur les risques vise à fournir sous forme de tableaux de bord à toutes les parties prenantes à la gestion des risques, une information synthétique, claire et concise sur les déterminants de base du management des risques (KEREBEL, 2007 : 45). Pour faire un reporting, selon Jimenez & Al (2008 :192), il faut :

- connaître le destinataire ou « client » de ce dernier, car la remontée d'information, sa synthèse et son traitement varient selon que le destinataire du reporting soit une direction générale, un responsable d'activités, un responsable des risques opérationnels ou autres du dispositif ;
- identifier les attentes vis-à-vis du reporting. S'agit-il d'une alerte pour action, d'un extrait pour prise de décision ou d'une simple information ? il s'agit de définir les objectifs auxquels l'on souhaite répondre, selon ses fonctions et responsabilités dans l'organisation ;
- dans certains cas (reporting réglementaire), fournir un canevas formaté.

#### **2.3.5. La phase de suivi**

La vérification de l'efficacité des plans d'actions est une phase importante du processus d'élaboration d'une cartographie des risques car c'est au cours de cette phase que peut être vérifié l'adéquation entre les risques et les contrôles mis en place (Jimenez & Al, 2008 : 116). Au cours de cette phase, les différentes actions de progrès mises en place sont suivies, et le rapport d'avancement du plan analysé (Maders & Al, 2006 : 230).

### **2.3.6. La phase d'actualisation**

Compte tenu de l'évolution des risques auxquels les entreprises sont confrontées, il est clair que la nécessité de faire une mise à jour régulière de la cartographie des risques s'impose. Ainsi, De Mareschal (2003 : 50) affirme « qu'il convient, en outre, pour une optimisation des résultats escomptés, de reprendre le processus de cartographies des risques en entier, au moins une fois par an, afin de permettre une gestion plus active des risques ».

## **2.4. Diagnostic d'une démarche d'élaboration de cartographies des risques**

Dans cette partie nous allons dans un premier lieu préciser la notion de diagnostic et dans un second lieu faire une synthèse des démarches généralement utilisées pour le diagnostic.

### **2.4.1. Définition du concept diagnostic**

Un diagnostic est ce qui appartient ou est en rapport avec la diagnose. De cette interprétation, le diagnostic se réfère à l'action et à l'effet de diagnostiquer c'est-à-dire recueillir et analyser des informations/données dans le but d'évaluer des problèmes de toute sorte.

En plus d'avoir un sens relevant du domaine médical, le diagnostic a un autre sens plus général. Ainsi, selon Degos (2010 : 5), le diagnostic « c'est une prévision, une hypothèse tirée de signes, ou encore la description des aspects caractéristiques d'une situation. ».

Dans Larousse (2006 : 122), le diagnostic est défini comme un « jugement porté sur une situation, sur un état. ». A partir de ces différentes définitions nous pouvons dire que le diagnostic est un raisonnement qui nécessite des observations sur un système. Ces observations peuvent ainsi révéler les forces et faiblesses de ce système.

### **2.4.2. Démarche de diagnostic**

Trouver la meilleure solution d'un système, c'est identifier ses forces et faiblesses et apporter des correctifs. L'identification de ses forces et faiblesses passe inéluctablement par l'analyse SWOT qui signifie selon Krogerus & al (2012 : 14), « identifier les Forces (Strengths), les Faiblesses (Weaknesses), les Opportunités (Opportunities) et les Menaces (Threats) d'un projet ». C'est un outil très prisé par les analystes (les consultants, les économistes) et souvent même exigé par les décideurs car il fait un parfait résumé pour une meilleure prise de décisions. Mettre l'accent sur les forces et faiblesses d'un système, c'est s'intéresser aux facteurs internes liés à ce système. Toutefois quand l'accent est mis sur les opportunités et menaces ce sont les facteurs externes liés à ce système qui sont considérés.



Figure 3 : Matrice SWOT



Source : Google image

La revue de la littérature n'a pas permis de trouver une démarche spécifique de diagnostic d'une cartographie des risques, cependant le modèle qui vient d'être présenté pourra lui être appliqué.

## Conclusion

Ce chapitre que nous venons d'aborder nous a permis de mieux cerner les différentes approches méthodologiques d'élaboration de cartographies des risques et comprendre comment faire un diagnostic. Dans le chapitre qui va suivre nous aborderons la méthodologie d'étude de notre étude.

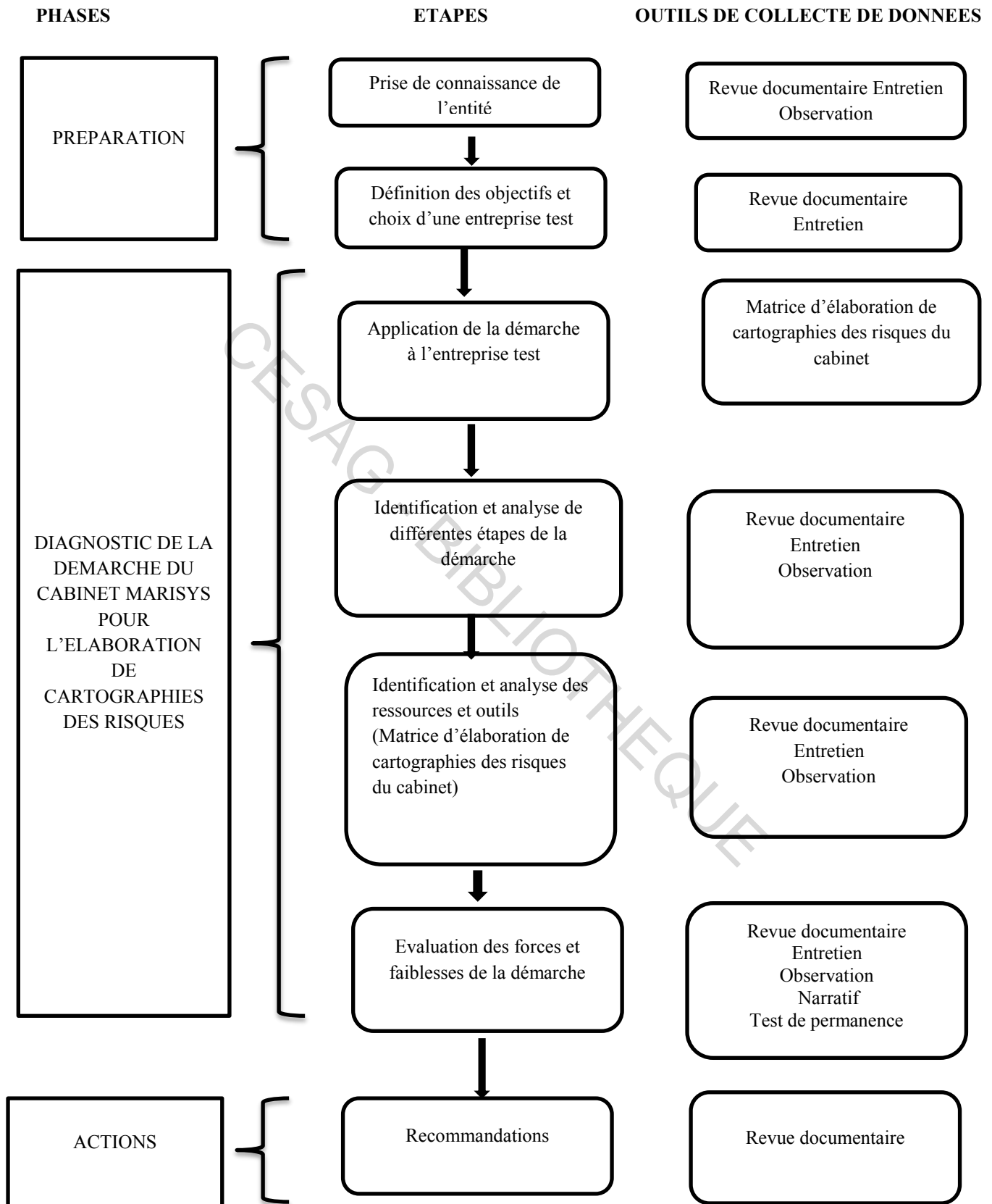
## CHAPITRE 3 : METHODOLOGIE DE L'ETUDE

La revue de littérature nous a permis de mettre en exergue la notion de cartographies des risques et les différentes démarches d'élaboration de cartographies des risques. Dans ce chapitre nous présenterons notre modèle d'analyse qui aidera à mieux aborder la partie pratique de notre mémoire. En ce qui concerne notre étude nous allons nous focaliser sur les forces et faiblesses de la démarche d'élaboration de cartographies des risques de MARISYS.

### 3.1. Modèle d'analyse

Cette section va nous permettre de décrire la démarche de résolution de notre problème, aussi les outils utilisés pour diagnostiquer la démarche du cabinet pour l'élaboration d'une cartographie des risques. Dans notre travail de diagnostic de la démarche d'élaboration de cartographies des risques, il s'agira de faire une analyse après description de cette démarche et de ressortir les forces et faiblesses.

Figure 4 : Modèle d'analyse



Source : nous même

## **3.2. Outils de collecte et d'analyse de données**

L'objectif de cette partie est de présenter les outils de collecte et d'analyse des données relatifs à l'élaboration d'une cartographie des risques par le cabinet MARISYS.

### **3.2.1. Outils de collectes de données**

La compréhension de la démarche du cabinet se fera grâce aux outils de collecte de données comme la revue documentaire, l'observation, l'interview.

#### **3.2.1.1. Revue documentaire**

La revue documentaire permet d'exploiter les documents du cabinet afin d'en extraire un maximum utile à la compréhension de la démarche du cabinet pour l'élaboration d'une cartographie des risques. Cette revue documentaire s'est faite sur la base de ce qui se pratique sur le terrain. Pour cela nous avons consulté les documents internes du cabinet comme les rapports de mission, des documents permanents, les plans de mission, les rapports d'activités etc. et divers documents fournis par le cabinet. Cela a permis d'avoir une meilleure compréhension sur les pratiques d'élaboration d'une cartographie des risques.

#### **3.2.1.2. L'observation**

Nous avons effectué des observations et cela grâce au travail quotidien du cabinet et aussi une mission réalisée par le cabinet pour l'élaboration d'une cartographie des risques et plan d'audit basé sur les risques pour mieux comprendre les différentes étapes d'élaboration d'une cartographie des risques par le cabinet et ceux jusqu'à la rédaction du rapport et la finalisation de la mission.

#### **3.2.1.3. L'interview**

Une interview est une conversation suivie avec une ou plusieurs personnes dans le but de la ou les interroger sur ses ou leurs actes/idées/projets, afin d'en publier ou diffuser le contenu. Il s'agit donc de l'action d'interroger (l'interviewer) et d'être interrogé (l'interviewé). Ainsi pour la résolution de notre problème nous nous sommes entretenus avec l'associé gérant cabinet MARISYS Sénégal et ses collaborateurs ce qui nous a permis de comprendre les activités au sein du cabinet et d'avoir une idée claire de la démarche du cabinet pour l'élaboration d'une cartographie des risques.

### 3.2.2. Outils d'analyses de données

#### 3.2.2.1. Le narratif

La narration désigne un récit détaillé, autrement dit la description pure et simple des différentes activités nécessaires à l'élaboration de la cartographie des risques, ce qui nous a permis d'analyser les différentes phases d'élaboration d'une cartographie des risques.

#### 3.2.2.2. Test de permanence

Selon Maders & Masselin (2014 :63) le test de permanence vise à s'assurer que les opérations sont bien traitées dans la réalité conformément à ce qui a été décrit lors des entretiens. Lorsque ce test est réalisé de manière systématique sur l'ensemble d'une période et/ou pour toutes les classes d'acteurs concernés dans l'objectif de s'assurer par sondage que toutes les opérations ont été effectivement traitées comme décrit, on parle alors de tests de permanence.

Il s'agira pour nous de s'assurer que les opérations pour l'élaboration de la cartographie des risques par le cabinet sont réalisées tels que décrites pendant les entretiens.

## Conclusion

Ce chapitre nous a permis de présenter notre modèle d'analyse ce qui servira de guide pour notre travail. Nous avons aussi mentionné de façon précise les outils et les méthodes pour répondre aux objectifs de notre travail. Ce modèle a été élaboré avec une prise en compte de la complexité de notre travail.

## CONCLUSION DE LA PREMIERE PARTIE

L'objectif de cette première partie était de faire une revue de la littérature devant nous permettre d'avoir des éléments écrits sur notre travail, de construire notre modèle d'analyse visant une meilleure compréhension de la démarche d'élaboration de la cartographie par notre cabinet d'accueil, le modèle d'analyse, un instrument qui identifie les différents phases du processus de gestion des risques, nous aidera à collecter les données, les analyser, à présenter nos résultats et à faire des recommandations.

CESAG - BIBLIOTHEQUE

**DEUXIEME PARTIE : CADRE PRATIQUE DE L'ETUDE**

CESAG - BIBLIOTHEQUE

## INTRODUCTION DE LA DEUXIEME PARTIE

Dans la première partie, nous avons abordé le cadre conceptuel de l'élaboration de cartographies des risques et la revue de littérature sur les différentes démarches d'élaboration d'une cartographie des risques. La revue de la littérature sur la démarche de diagnostic a aussi été présentée. Dans la deuxième partie qui va suivre, il sera question de mettre en pratique notre méthodologie de recherche évoquée dans la première partie afin de diagnostiquer la démarche d'élaboration d'une cartographie des risques au cabinet MARISYS.

Pour y arriver nous allons dans un premier chapitre faire la présentation du cabinet et dans un deuxième, décrire la démarche du cabinet pour l'élaboration d'une cartographie des risques et enfin terminer par le troisième chapitre qui sera consacré à l'analyse des forces et faiblesses de cette démarche afin de faire des recommandations dans le but de contribuer à son amélioration.



## CHAPITRE 4 : PRESENTATION DE MARISYS SENEGAL

Pour une bonne connaissance de notre terrain d'étude, nous parlerons, dans ce chapitre de la description du cabinet MARISYS SENEGAL, cette description mettra en exergue l'historique, les missions, les objectifs assignés au cabinet, son organisation et ses activités.

### 4.1. Présentation du cabinet MARISYS Sénégal

MARISYS Sénégal est un cabinet de conseil et d'assistance des entreprises et organisation du secteur public et privé. Il apporte à ses clients innovation et expertise pour contribuer à leur dynamisme. Il est partenaire d'un réseau de compétences confirmés en Europe et en Afrique et disposant de l'expérience des projets menés dans des environnements complexes, sensibles et critiques, notamment pour le secteur public et privé, dans l'administration, l'industrie les services et la sécurité. Cet atout lui permet d'accompagner durablement ses clients dans leurs activités en répondant à leurs exigences de transformation.

#### 4.1.1. Historique du cabinet

MARISYS est un réseau international de cabinets présent en France et en Afrique, notamment au Sénégal, en Côte d'Ivoire, au Togo, en RDC, etc.

MARISYS Sénégal a ouvert ses bureaux au Sénégal en 2015 et dirigé par Monsieur Mor Badiane TINE associé gérant avec un titre de société à responsable limité au capital de 1.000.000 FCFA.

#### 4.1.2. Missions du cabinet MARISYS

Le cabinet MARISYS se fixe pour mission d'offrir aux entreprises un service qualité dans le domaine de conseil.

#### 4.1.3. Activités du cabinet MARISYS

MARISYS Sénégal a pour objet, en tout pays et plus particulièrement au Sénégal, toutes opérations concernant :

- Le conseil et l'appui dans la conception et la mise en place de systèmes intégrés de management, du contrôle interne et de gestion des risques :
  - conception et mise en place de manuel des procédures administratives, financières et comptables ;
  - mise en place de systèmes comptable ;

- élaboration de cartographies des risques, plan de mitigation et plan d'audit interne basé sur les risques ;
  - élaboration de manuel d'audit interne ;
  - appui à l'élaboration et à la mise en place d'un service d'audit interne ou de contrôle de gestion.
- La formation dans les domaines du management et du contrôle :
- comptabilité générale et analytique ;
  - audit et contrôle interne ;
  - contrôle de gestion et gestion et gestion budgétaire ;
  - cartographie et management des risques ;
  - gestion et audit de projets.
- Tous conseils et services informatiques :
- innovation et expertise pour contribuer aux dynamismes de ses clients. Toutes activités concernant les projets menés dans des environnements complexes sensibles et critiques, notamment pour les secteurs publics et privés, dans l'administration, l'industrie, le service et la sécurité.
- En matière de services liés à l'informatique et l'internet :
- conception et mise en place de systèmes intégrés de management, du contrôle interne et de gestions des risques entités ;
  - conseils en technologie de l'information ;
  - services de gestion de projets informatiques ;
  - conseils en sécurité informatique ;
  - intégration de système de technologies de l'information ;
  - validation de systèmes informatiques ;
  - audit de Conseil en sécurité informatique (physique et logique)
  - services de certification de vérification de contenus ;
  - conseils et services pour portails internet ;
  - tierce maintenance du logiciel ;
  - intégration, développement et maintenance de logiciels libres ;
  - sous-traitance informatique (infogérance, facilités management)
  - services de sécurité des réseaux ;
  - formations professionnelles et programmes de recyclage pour affaires, le commerce et de l'administration ;

- logiciels sur spécification client, sociétés de services et d'ingénierie informatique.
- Tous produits et services concernant :
  - centrale et matériel pour réseaux de télécommunication ;
  - systèmes intégrés informatiques sur spécification client ;
  - systèmes d'exploitation, logiciels systèmes et de développement ;
  - logiciels d'application bureautique, commerciale, professionnelle, comptable et financière ;
  - progiciels, logiciels d'application ;
  - services de traitement de l'information et de saisie de données ;
  - services liés à l'informatique et à internet ;
  - conseils en sécurité industrielle et en présentation des accidents ;
  - conseils en sécurité industrielle et en prévention des accidents.

En plus généralement, toutes opérations industrielles, commerciales, financières, mobilières et immobilières pouvant se rattacher directement ou indirectement à l'objet social et à tous objets similaires ou connexes de nature à favoriser son extension ou son développement.

#### **4.2. Organisation du cabinet MARISYS**

Le cabinet Marisys fonctionne sous la direction d'un directeur associé expert dans le domaine de la gestion des risques de l'audit et du contrôle interne, et plusieurs collaborateurs experts de hauts niveaux dans le domaine de la gestion (Annexe 1)

##### ➤ Directeur Associé

Le cabinet Marisys Sénégal est dirigé par Monsieur Mor Badiane TINE auditeur ayant servi dans plusieurs pays de la sous-région comme le Burkina Faso avec plus de 25 ans d'expérience. Avec les équipes dont il a la charge, il sera amené à :

- accompagner et développer le travail des consultants
- effectuer des interventions auprès des clients
- garantir le bon déroulement des missions jusqu'à la réalisation de l'opération

Et toute autre mission en sa charge.

➤ Chef de Mission

Autonome, il a la responsabilité d'un portefeuille clients et encadre une équipe d'Auditeurs assistant, Il intervient sur des missions non récurrentes et aborde des problématiques d'un certain niveau technique. Au quotidien, il assure un rôle de conseil et de suivi auprès de ses clients dans le but de bien appréhender leur environnement, comprendre leur problématique et intervenir avec le plus de réactivité et de pertinence possible dans les conseils apportés.

➤ Responsable formation

Il est responsable organisationnel et exécutif des formations inter-entreprises et extra-entreprises organisés par le cabinet dans ses domaines de compétences du cabinet.

➤ Auditeurs Assistants

L'assistant audit participe à l'exécution des missions du cabinet : il réalise les travaux confiés par le responsable de la mission et assiste l'auditeur dans le cadre du programme de travail. Il réalise ces travaux dans le respect des délais définis. Il participe au développement de l'image du cabinet auprès des clients.

## **Conclusion**

Ce chapitre nous a permis d'avoir une meilleure connaissance du cabinet MARISYS Sénégal sans oublier son historique, ses missions et son activité. MARISYS Sénégal a depuis sa création progressivement accru le nombre de ses missions. Dans l'optique d'une amélioration continue il s'est fixé de nouveaux objectifs pour le développement de son activité. Dans le chapitre suivant nous procéderons au diagnostic de la démarche du cabinet Marisys par l'application de cette démarche à un cas X des clients du cabinet.

## CHAPITRE 5 : DESCRIPTION DE LA DEMARCHE D'ELABORATION D'UNE CARTOGRAPHIE DES RISQUES D'UNE DIRECTION DU SYSTEME D'INFORMATION

Dans ce chapitre il s'agira pour nous de décrire la démarche du cabinet MARISYS pour l'élaboration d'une cartographie des risques, par la mise en application de cette démarche dans la direction du système d'information d'une entreprise cliente du cabinet, dont nous nous gardons de taire le nom pour des raisons de confidentialité.

### 5.1. Présentation des différentes phases de l'approche MARISYS

L'élaboration d'une cartographie des risques selon la démarche du cabinet MARISYS suit un ensemble de phases et de processus. Dans cette section il s'agira d'aborder ces différentes phases et processus.

#### 5.1.1. Phase de planification de la mission

Selon la démarche du cabinet le processus de planification doit porter sur la définition des objectifs et du périmètre, le calendrier de la mission, les prévisions d'effectifs et les budgets financiers. Dans cette phase de la démarche, il s'agira de partir des objectifs de gestion et découper la structure en ensembles homogènes (processus, sous processus et à l'intérieur de chaque processus, les entités.).

##### 5.1.1.1. Prise de connaissance dans l'entité

Pour mener à bien une mission de cartographie des risques, le cabinet MARISYS cherche en premier lieu à comprendre les objectifs de l'entité, les tâches effectuées dans le domaine examiné qui visent à atteindre ces objectifs, ainsi que les mécanismes de pilotage des performances et de mesure de la réussite.

La simple prise de connaissance des processus dans l'entité n'étant pas suffisante et pouvant présenter des risques quant à la qualité de l'interprétation qui en est faite. Le cabinet, pour avoir une information fiable, se réfère aux documents sources, rassemblés dans un dossier unique pour toutes les entités.

La constitution du dossier de référence (dossier permanent) peut passer par l'obtention des informations de base ci – après :

- la définition de la mission de l'entité, les objectifs et les plans (missions, objectifs stratégiques, opérationnels, indicateurs de performance) ;

- des informations sur l'organisation par exemple, l'organigramme général et détaillé, les descriptions de poste, le nombre et les noms des collaborateurs, les collaborateurs occupant des postes-clé, les manuels de procédures et de politique, ainsi que les détails sur les derniers changements d'organisation, y compris les changements importants de façon générale ;
- des informations budgétaires, des résultats des opérations, et des données financières sur l'activité à auditer ;
- les dossiers d'audits précédents ;
- des résultats d'autres audits, y compris ceux des auditeurs externes, terminés ou en cours ;
- des dossiers pour déterminer des problèmes potentiels importants ;
- la littérature technique faisant autorité pour l'activité.

La constitution de ces dossiers nécessite des relations préliminaires avec l'entité, notamment, les différents services de doctrine ou d'élaboration des directives, normes internes et procédures. Il est en particulier essentiel d'obtenir la validation des dossiers par les directeurs opérationnels concernés afin d'être certains de la référence qu'utiliseront les auditeurs.

La constitution de ces dossiers est un moment important de la démarche d'élaboration de la cartographie, elle permet la formalisation de la lettre de mission.

Un atelier d'échange et de cadrage avec tous les acteurs impliqués (managers, opérationnels) peut être organisé pour permettre aux participants de :

- comprendre et s'accorder sur les concepts, les techniques et les outils ;
- comprendre comment les organisations structurent leurs activités pour atteindre leurs objectifs ;
- appréhender les différents rôles attribués aux managers et à l'audit interne dans le management des risques dans une organisation ;
- comment identifier les processus clés d'une organisation ;
- maîtriser le concept processus et savoir le documenter ;
- comprendre les risques de base auxquels sont confrontées les organisations ;
- identifier et évaluer les principaux risques pesant sur la réalisation des objectifs de l'organisation et leur relation avec les processus ;
- savoir élaborer un univers d'audit pour une organisation, proposer après évaluation des risques résiduels, un plan de mitigation.

#### 5.1.1.2. Détermination des objectifs et périmètre de la mission : la lettre de mission

La mission d'élaboration ou d'actualisation de la cartographie des risques conduite par l'audit interne entre dans la catégorie des missions mixtes d'assurance et de conseil qui vise la palette d'objectifs suivants :

- évaluer indépendamment d'un processus ou de contrôles ;
- donner des conseils aux managers à tous les niveaux de l'organisation sur la manière de documenter et de regrouper leurs évaluations des risques et des contrôles ;
- faciliter les autoévaluations :
  - l'évaluation par la direction générale des risques qui menacent l'organisation dans son ensemble ;
  - l'évaluation par les propriétaires des processus des risques qui menacent leurs activités.
- mener des formations en interne :
  - renseigner les audités et leur hiérarchie sur les nouvelles lignes directrices qui font autorité sur la gouvernance d'entreprise, le management des risques et le contrôle ;
  - informer les propriétaires des processus et le personnel sur les concepts fondamentaux que sont la gouvernance d'entreprise, le management des risques et le contrôle.

#### 5.1.1.3. Elaboration d'un programme de travail et allocation des ressources

Une planification détaillée avec affectation des ressources est faite. Un **programme de travail formel** présentant les principales activités du processus de la mission et tout jugement formulé concernant les objectifs et le périmètre de la mission.

En se fondant sur les activités à réaliser au cours de la mission, l'auditeur doit identifier et désigner les membres du personnel correspondant au niveau d'expérience et de compétence approprié, afin que la mission puisse être menée dans les temps et avec efficacité.

Il y a lieu également d'estimer les **moyens logistiques et financiers** nécessaires à la correcte réalisation de la mission (Bureau, Équipements, Fournitures de bureaux).

#### 5.1.1.4. La réunion d'ouverte

Fortement recommandée, conduite par le chef de mission, elle réunit la hiérarchie supérieure et les opérationnels de la structure (futurs interlocuteurs) et a pour objectif de préciser avec ces derniers :

- l'objet de la mission,
- les attentes prioritaires des audités,
- le cadre et les limites,
- la date de début et la durée prévisionnelle,
- le ou les structures concernées,
- la composition de l'équipe d'audit,
- l'approche et les outils,
- l'ordre de passage
- si cela est nécessaire, les moyens à mettre à la disposition des auditeurs (personnel, véhicules, accès aux outils informatiques).

La réunion d'ouverture est sanctionnée par un procès-verbal (PV réunion d'ouverture).

#### 5.1.2. Phase de formation

Pour un transfert de connaissance et culture du risque après la phase de planification, pour commencer la phase sur le terrain le cabinet MARISYS organise une séance de formation suivie d'un cas pratique d'élaboration de la cartographie des risques d'une durée de trois (03) jours minimums.

- l'approche du cabinet étant participative avec **une démarche de changement** :
  - en changeant la confiance souvent aveugle envers le monde dans lequel on travail (pessimisme professionnel : remise en cause perpétuelle) ;
  - en changeant le savoir-faire par l'apport une méthodologie d'analyse professionnelle des risques ;
  - en instituant une culture de partage (des connaissances, des savoir-faire) ;
  - en créant une synergie de groupe collaborant à une œuvre commune (référentiel de CI) ;
  - en amenant tous les acteurs à prendre leurs responsabilités, dans une culture d'autogestion et d'auto suggestion par la recherche de solutions adaptées ;



### 5.1.3. Phase de réalisation

Cette phase de réalisation sur le terrain se fait en 15 étapes à savoir :

- inventaire avec les managers et les opérationnels des missions et des objectifs de structures.
  - ici pour l'exemple le cabinet à fait un inventaire des objectifs et missions de la direction du système d'information (DSI) ;
- recensement de l'ensemble des processus et des informations ;
  - le cabinet procède ici au recensement de l'ensemble des processus de l'entité avec l'ensemble des managers et des informations sur ces processus.

- travail de groupe de description chronologique :

Le cabinet aussi faire ressortir

- des objectifs stratégiques ;
- des objectifs opérationnels ;
- des activités et tâches (chronologique).

De la direction du système d'information.

Processus concernés
Sous processus concernés

De ces trois points le cabinet MARISYS a ressorti le tableau ci-dessous grâce à sa matrice d'élaboration de cartographies des risques.

Tableau 3 : Représentation des sous processus de la DSI

<b>Mettre en place et gérer le système d'information (Système informatique, télécommunication, solutions métiers)</b>	
<b>1</b>	Définir la politique informatique de l'entreprise (SDI, GSI, USI, PA)
<b>2</b>	Superviser tous les projets d'acquisition des ressources informatiques suivant le SDI
<b>3</b>	Superviser tous les projets de déploiement des ressources informatiques (matérielles et logicielles) et télécoms (Réseaux Informatiques et Téléphonie)
<b>4</b>	Intégrer la solution logicielle (spécifique ou standard)
<b>5</b>	Assurer la formation des utilisateurs du système d'information
<b>6</b>	Veiller à la sécurité et à la disponibilité du système information
<b>7</b>	Veiller à l'assistance des utilisateurs (Support)

Source : nous-même inspiré de la matrice MARISYS SENEGAL

- Identifier en groupe les risques potentiels pesant sur les tâches (facteurs d'empêchements internes et externes) identification basée sur les check-lists, analyse des faits historiques, analyse de l'environnement, analyse des activités etc.

Dans cette étape le cabinet avec l'ensemble des managers énumère les risques potentiels pesant sur activités, processus, objectifs.

Ainsi pour notre exemple celle de la DSI il peut ressortir des risques suivant par processus ou objectifs de la DSI, présenter dans un tableau à l'aide de la matrice MARISYS (Annexe2) :

Tableau 4 : Risques potentiels identifiés par processus

	1	2	3	4	5
<b>Processus</b>	<b>Définir la politique informatique de l'entreprise (SDI, GSI, USI, PA)</b>	<b>Superviser tous les projets d'acquisition des ressources informatiques suivant le SDI</b>	<b>Superviser tous les projets de déploiement des ressources informatiques</b>	<b>Intégrer la solution logicielle (spécifique ou standard)</b>	<b>Veiller à la sécurité et à la disponibilité du système information</b>
<b>Risques potentiels</b>	Définition d'une politique inadaptée aux missions de l'entreprise	Acquisition de ressources inappropriées	Défaillance du déploiement opérationnel de la ressource informatique	Mauvaises spécifications techniques	Défaillance matérielle ou logicielle
	Absence de politique informatique	Retard dans l'acquisition des ressources informatiques	Anomalies non détectées lors du déploiement	Non adhésion (hostilité) à la solution proposée	Comportement inapproprié d'un utilisateur (Non-respect des mesures de sécurités)
	Définition d'une politique inadaptée à l'organisation interne (organigramme)	Défaillance du fournisseur	Mauvais paramétrage	Retard dans le processus d'intégration de la solution	Intrusions
	Absence de charte informatique	Ressources informatiques livrées défectueuses	Retard dans le déploiement	Solution inadaptée aux besoins des utilisateurs	Indisponibilité du système
					Perte de données
					Usurpation d'identité
					Diffusion non autorisée de l'information
					Infection par un logiciel malveillant

Source : nous-même inspiré de la matrice MARISYS

Après identification des risques le cabinet procède à la sélection de trois (03) jugés pertinents pour les sous processus concernés avec l'ensemble des managers ou acteurs du processus concernés.

Cependant dans le cadre de notre mémoire pour des raisons de commodité de gestion du nombre de pages nous allons nous limiter à cinq (05) sous processus et n'analyser que deux (02) risques jugés majeurs par sous processus.

Tableau 5 : Risques potentiels retenus pour analyse

	1	2	3	4	5
<b>Processus</b>	<b>Définir la politique informatique de l'entreprise (SDI, GSI, USI, PA)</b>	<b>Superviser tous les projets d'acquisition des ressources informatiques suivant le SDI</b>	<b>Superviser tous les projets de déploiement des ressources informatiques</b>	<b>Intégrer la solution logicielle (spécifique ou standard)</b>	<b>Veiller à la sécurité et à la disponibilité du système information</b>
<b>Risques Potentiels</b>	Définition d'une politique inadaptée aux missions de l'entreprise	Acquisition de ressources inappropriées	Anomalies non détectées lors du déploiement	Mauvaises spécifications techniques	Perte de données
	Définition d'une politique inadaptée à l'organisation interne (organigramme)	Retard dans l'acquisition des ressources informatiques	Retard dans le déploiement	Solution inadaptée aux besoins des utilisateurs	Indisponibilité du système

Source : nous-même inspiré de la matrice MARISYS

- Déterminer la catégorie ou typologie de risques (sur 17 types modulables) :  
ici le cabinet procède à une détermination de la typologie des risques retenus parmi les typologies présentes dans sa Matrice MARISYS.

Tableau 6 : Les différents types de risques

Type de risque			
N°		N°	
1	Risque Economique	11	Risque d'Image /réputation
2	Risque Stratégique	11	Risque d'intégrité
3	Risque Financier	12	Risque de Défaillance
4	Risque Opérationnel	13	Risque d'approvisionnement
5	Risque Informatique	14	Risque Environnemental
6	Risque Ressource Humaine	15	Risque démographique
7	Risque de fraude, corruption, détournement	16	Risque de projet
8	Risque qualité du service	17	
9	Risque qualité de l'information		
10	Risque Juridique		

Source : nous-même inspiré de la matrice MARISYS

- Identifier collectivement les causes probables (composant du contrôle interne).
- Identifier collectivement les conséquences probables de la réalisation du risque.

Il s'agira pour ces deux étapes ci-dessous d'identifier quelques causes pouvant être à la source de ces risques et conséquences probables que ces risques pourraient engendrer.

Cette partie après avoir sélectionné deux (02) risques jugés pertinent par les managers nous identifierons quelques causes et conséquences probables qui pourraient engendrer ces risques.

Tableau 7 : Identification des causes et des conséquences probables

Réf	Missions/objectifs /activités	Risques Retenus	Types de risques	Causes Probables	Conséquences Probables
1	<b>Définir la politique informatique de l'entreprise (SDI, GSI, USI, PA)</b>	Définition d'une politique inadaptée aux missions de l'entreprise	Risques stratégiques	1- Absence de visibilité des missions de l'entreprise 2- Manque d'expérience 3- Manque de budget ou Prévision erronée 4-Insuffisance ou manque de compétence des ressources humaines 5- Absence de recensement des besoins 6- Faible implication des agents	1- Mauvaise politique 2- Politique inefficace 3- Perte financière (Investissement inapproprié) 4- Perte de temps 5- Atteinte de l'image de l'entreprise 6-Manque d'optimisation des services
		Définition d'une politique inadaptée à l'organisation interne (organigramme)	Risques stratégiques	1- Absence d'organigramme 2- Organigramme en perpétuel modification 3- Mauvaise définition de l'organigramme 4-Mauvaise application de l'organigramme 5- Inaccessibilité de l'organigramme	1- Mauvaise politique 2- Politique inefficace 3- Perte financière (Investissement inapproprié) 4- Perte de temps 5- Atteinte de l'image de l'entreprise 6-Manque d'optimisation des services
2	<b>Superviser tous les projets d'acquisition des ressources informatiques suivant le SDI</b>	Acquisition de ressources inappropriées	Risques d'approvisionnements	1-Mauvaise définition des caractéristiques techniques 2- Disfonctionnement lors de la réception 3- Mauvais recensement des besoins 4- Mauvaise foi du fournisseur 5- Mauvaise préparation des dossiers d'appel d'offre	1- Perte Financière 2- Perte de temps 3- Inefficacité dans les missions quotidiennes 4-Ressources incompatibles 5- Ressources inexploitable

**Diagnostic de la démarche d'élaboration de cartographies des risques au cabinet MARISYS Sénégal**

		Retard dans l'acquisition des ressources informatiques	Risques d'approvisionnements	<ul style="list-style-type: none"> <li>1- Absence de budget</li> <li>2- Réaménagement budgétaire défavorable</li> <li>3- Absence d'inscription dans le PPM</li> <li>4- Défaillance du fournisseur</li> <li>5- Manque de respect des procédures de Passation des marchés</li> <li>6- Présence de Contentieux et Recours auprès d'ARMP</li> </ul>	<ul style="list-style-type: none"> <li>1- Perte Financière</li> <li>2- Perte de temps</li> <li>3- Inefficacité dans les missions quotidiennes</li> <li>4- Ressources incompatibles</li> <li>5- Ressources inexploitable</li> <li>6- Absence de déploiement de ressources</li> </ul>
3	<b>Superviser tous les projets de déploiement des ressources informatiques</b>	Anomalies non détectées lors du déploiement	Risques de défaillance	<ul style="list-style-type: none"> <li>1- Tests non effectués</li> <li>2- Absence de rigueur</li> <li>3- Absence de formation qualifiée sur les ressources à déployer</li> <li>4- Absence de compétences requises pour le suivi du déploiement</li> </ul>	<ul style="list-style-type: none"> <li>1- Dysfonctionnements de la ressource déployée</li> <li>2- Absence d'exploitation de la ressource</li> <li>3- Utilisation non optimale de la ressource</li> <li>4- Perte de temps</li> <li>5- Contentieux avec le fournisseur</li> <li>6- Perte financière</li> <li>7- Atteinte de l'image du service DSI</li> <li>8- Atteinte de l'image de l'entreprise</li> </ul>

**Diagnostic de la démarche d'élaboration de cartographies des risques au cabinet MARISYS Sénégal**

		Retard dans le déploiement	Risques opérationnels	<ul style="list-style-type: none"> <li>1- Mauvaise planification du déploiement</li> <li>2- Absence de dispositif nécessaire au déploiement</li> <li>3- Panne technique (Electricité, réseau, ...)</li> <li>4- Absence de planification du déploiement</li> <li>5- Retard dans la délivrance de l'Ordre de Service</li> <li>6- Non-conformité technique de la ressource à déployer</li> <li>7- Indisponibilité des acteurs</li> </ul>	<ul style="list-style-type: none"> <li>1- Service non opérationnel</li> <li>2- Perturbations dans la Planification des missions de l'entreprise</li> <li>3- Atteinte de l'image du service informatique</li> <li>4- Personnel non opérationnel</li> <li>5- Perte de temps</li> <li>6- Perte financière</li> <li>7- Atteinte de l'image de l'entreprise</li> </ul>
4	<b>Intégrer la solution logicielle (spécifique ou standard)</b>	Mauvaises spécifications techniques	Risques de projets	<ul style="list-style-type: none"> <li>1- Absence de collaboration des acteurs</li> <li>2- Absence de Termes De Références (TDR)</li> <li>3- Mauvaise élaboration des TDR</li> <li>4- Manque de culture informatique</li> <li>5- Absence de formations certifiantes sur les nouvelles approches technologiques</li> <li>6- Absence de veille technologique</li> </ul>	<ul style="list-style-type: none"> <li>1- Absence de solutions logicielles</li> <li>2- Solutions logicielles inadaptées</li> <li>3- Solutions logicielles inexploitable</li> <li>4- Perte de crédibilité</li> <li>5- Lenteur dans l'exécution des tâches quotidiennes</li> <li>6- Perte de temps</li> <li>7- Perte financière</li> <li>8- Services non opérationnel</li> </ul>



Diagnostic de la démarche d'élaboration de cartographies des risques au cabinet MARISYS Sénégal

		Solution inadaptée aux besoins des utilisateurs	Risques de projets	<ul style="list-style-type: none"> <li>1- Mauvais recensement des besoins</li> <li>2- Bogue dans la solution logicielle proposée</li> <li>3- Absence de capacité d'évolution de la solution logicielle</li> <li>4- Complexité des fonctions proposées par la Solution logicielle</li> <li>5- Absence de formation sur la solution</li> </ul>	<ul style="list-style-type: none"> <li>1- Perte Financière</li> <li>2- Perte de temps</li> <li>3- Absence d'automatisation des procédures (manuel)</li> <li>4- Absence de qualité de service</li> <li>5- Absence d'intégrité des données</li> </ul>
5	<b>Veiller à la sécurité et à la disponibilité du système information</b>	Indisponibilité du système	Risques opérationnels	<ul style="list-style-type: none"> <li>1- Pannes de la machine serveur ou de l'autocommutateur</li> <li>2- Délestage électrique</li> <li>3- Défaillance climatisation de la salle serveur</li> <li>3- Défaut de paiement (Ligne téléphonique, Internet ...)</li> <li>4- Problèmes d'interconnexions</li> <li>5- Absence de système de secours (Backup énergie, ligne de secours, câblage, ...)</li> <li>6- Absence de politique de sauvegarde pour assurer la reprise après panne</li> <li>7- Sinistre (Infiltration d'eau dans la salle serveur (Crue), tremblement de terre, etc.,)</li> <li>8- Incendie</li> <li>9- Sabotage ou Cambriolage de ressources essentielles dans les locaux techniques</li> <li>10- Intrusion, Piratage (Ransomware, etc.,)</li> </ul>	<ul style="list-style-type: none"> <li>1- Arrêt des services informatiques</li> <li>2- Arrêt des services téléphoniques</li> <li>3- Absence de satisfaction des usagers du service public</li> <li>4- Perte Financière</li> <li>- Atteinte à l'image de l'entreprise</li> <li>7- Perte de temps</li> <li>8- Perte de ressources matérielles</li> <li>9- Blocage du fonctionnement de l'entreprise</li> <li>10- Non-exécution des missions</li> <li>11- Exposition à des sanctions sur la législation informatique en vigueur</li> <li>12- Usurpation d'identité</li> </ul>

**Diagnostic de la démarche d'élaboration de cartographies des risques au cabinet MARISYS Sénégal**

		Perte de données	Risques opérationnels	<ul style="list-style-type: none"> <li>1- Dommages matériels ou périphériques (Disque dur défectueux, Instabilité de tension, décharge, Surchauffe, etc.,)</li> <li>2- Erreurs humaines (Ecrasement ou suppression de fichiers accidentels, mauvaise manipulation, migration ou vol de données)</li> <li>3- Logiciels malveillants</li> <li>4- Prestataires mal intentionnés</li> <li>5- Catastrophe naturelle</li> </ul>	<ul style="list-style-type: none"> <li>2- Perte Financière</li> <li>3- Divulgence d'informations confidentielles</li> <li>4- Usurpation d'identité</li> <li>5- Vulnérabilité du système</li> <li>6- Corruption de fichiers</li> <li>7- Atteinte de l'image de l'entreprise</li> <li>8- Insatisfaction des usagers du service</li> <li>9- dégradation des images de l'entreprise</li> </ul>
--	--	------------------	-----------------------	---	--

Source : nous-même inspiré de la matrice MARISYS SENEGAL

- Évaluer et classer chaque scenario de risque inhérent (probabilité x impact) en appliquant les barèmes de la matrice MARISYS que voici pour évaluer le risque inhérent

Tableau 8 : Echelle d'évaluation de la probabilité de survenance du risque

<b>Echelle de probabilité des risques</b>					
<b>Niveau de probabilité</b>	<b>Très probable</b> <b>5</b>	<b>Probable</b> <b>4</b>	<b>Modérément probable</b> <b>3</b>	<b>Peu probable</b> <b>2</b>	<b>Rare</b> <b>1</b>
<b>Description</b>	Le risque s'est manifesté fréquemment et se manifestera très probablement plus d'une fois dans les 12 prochains mois	Le risque est courant. Il a une chance importante de se manifester au moins une fois dans les 12 prochains mois	Le risque a une chance au-dessus de la moyenne de se manifester au moins une fois dans les 3 prochaines années	Le risque est très peu fréquent, et peu probable de survenir dans les 3 prochaines années	Le risque est concevable mais il n'est susceptible de se manifester que dans circonstances extrêmes
<b>Critères qualitatifs (orientés fraudes, malveillances)</b>					
<b>Motivation</b>	Enrichissement personnel ou motifs idéologiques	Nuire à l'institution	Nuire à la bonne marche d'un service ou d'un processus	Nuire à la hiérarchie ou à ses collègues	Attirer l'attention (satisfaire son égo)
<b>Critères qualitatifs (orientés erreurs, incidents opérationnels)</b>					

Sensibilisation et compétence des personnels	Aucune culture du risque et du contrôle interne. Personnels de différents profils avec des compétences et une expérience faible. Absence de formation	Faible culture du risque et du contrôle interne. Personnels différents profils avec des compétences et ne expérience de base. Formation de base	Culture limitée du risque et du contrôle interne. Personnels de différents profils avec des compétences et une expérience standard. Formation standard	Forte culture du risque et du contrôle interne. Personnels de différents profils avec des compétences et une expérience avancée. Formation spécialisée	Très forte culture du risque et du contrôle interne. Personnels expérimentés avec une réelle expertise. Formation continue de haut niveau
--	---	--	--	--	---

Source : Matrice MARISYS

Tableau 9 : Echelle d'évaluation de l'impact de survenance du risque

Score – Evaluation	5- Critique	4- Majeur	3- Modéré	2- Mineur	1 - Non significatif
<b>Echelle d'impact sur l'objectif</b>					
Description de l'impact sur l'objectif	Risque ayant une importance critique sur la capacité d'atteinte de l'objectif de gestion	Risque ayant un impact relativement substantiel sur la capacité d'atteinte de l'objectif de gestion	Risque ayant un impact relativement modéré sur la capacité d'atteinte de l'objectif de gestion	Risque ayant un impact faible sur la capacité d'atteinte de l'objectif de gestion	Risque ayant un impact négligeable sur la capacité d'atteinte de l'objectif de gestion
<b>Echelle d'impact sur l'image</b>					
Durée de l'atteinte à l'image (vis-à-vis de l'opinion publique, d'organismes internationaux ou nationaux, des	Crédibilité gravement affectée à long terme (>3 ans)	Crédibilité gravement affectée à moyen terme (>1 an)	Crédibilité affectée à court terme (> 3 mois)	Crédibilité affectée à court terme (> 1 semaine)	Crédibilité affectée pendant moins d'une semaine

Partenaires Techniques et Financiers (PTF))					
<b>Echelle d'impact financier</b>					
Impact financier F CFA	> 10 000 000 CFA	1 000 000 à 10 000 000 CFA	100 000 à 1 000 000 CFA	10 000 à 100 000 CFA	< 10 000 CFA
<b>Echelle d'impact Humain</b>					
Impact humain (conditions sociales, de travail)	Impact ayant une importance critique sur les agents de l'entité (surcharge de travail, stress, démotivation, accidents de travail, maladies...).	Impact relativement substantiel sur les agents de l'entité (surcharge de travail, stress, démotivatio n, accidents de travail, maladies...).	Impact relativement modéré sur les agents de l'entité (surcharge de travail, stress, démotivation, accidents de travail, maladies...).	Impact faible sur les agents de l'entité (surcharge de travail, stress, démotivation, accidents de travail, maladies...).	Impact négligeable sur les agents de l'entité (surcharge de travail, stress, démotivation, accidents de travail, maladies...).
<b>Echelle d'impact sur les clients/partenaires</b>					
Impact sur les clients/ partenaires	Impact très important sur les parties prenantes externes : clients/usagers/ bénéficiaires, fournisseurs, PTF, investisseurs, etc.	Impact relativement significatif sur les parties prenantes externes : clients/usager s/bénéfici aires, fournisseurs , PTF, investisseur s, etc.	Impact significatif sur les parties prenantes externes : clients/usager s/bénéficiaire s, fournisseurs, PTF, investisseurs, etc.	Impact faible sur les parties prenantes externes : clients/usager s/bénéficiaire s, fournisseurs, PTF, investisseurs, etc.	Impact négligeable sur les parties prenantes externes : clients/usagers/bén éficiaries, fournisseurs, PTF, investisseurs, etc.

Source Matrice MARISYS

- Définir l'ensemble des bonnes pratiques de contrôle interne communément admises de maîtrise des risques qui devront exister.

Ici pour chaque risque le cabinet définit un ensemble de bonnes pratiques pour la maîtrise de chaque risque, ainsi pour notre exemple le cabinet avec l'ensemble des managers définissent un ensemble de bonnes pratiques.

- Evaluer l'efficacité des parades ou contrôle interne en place en appliquant les barèmes de MARISYS.

Après avoir défini les bonnes pratiques il faudra maintenant évaluer l'efficacité du contrôle interne en place et cela en se basant sur le barème dans la matrice MARISYS.

CESAG - BIBLIOTHEQUE

Tableau 10 : Evaluation du risque inhérent, identification des bonnes pratiques et des éléments clés du contrôle interne

Réf	Risques retenus	Risques Inhérents			Bonnes pratiques de CI de maitrise des risques	Eléments clés de contrôle interne existants et inexistantes	
		Impact de 1 à 5	Probabilité de 1 à 5	Score = P×I		Existants (forces apparentes)	Inexistants (faiblesses apparentes)
1	Définition d'une politique inadaptée aux missions de l'entreprise	5	4	20	1- Existence d'un schéma directeur informatique 2- Existence d'une fiche d'interviews et d'expression des besoins pour l'élaboration du schéma directeur informatique 3- Existence d'une charte informatique et signée 4- Existence d'une fiche de séparation des tâches 5- Possibilité de recourir aux services d'un consultant 6- Existence de personnel qualifié suffisant 7- Organisation d'ateliers de validation 8- Existence d'un plan d'actions 9- Validation des documents par le conseil de surveillance	1- Possibilité de recourir aux services d'un consultant 2- Existence d'un plan d'actions 3- Validation des documents par le conseil de surveillance	1- Absence d'un schéma directeur informatique 2- Inexistence d'une fiche d'interviews et d'expression des besoins pour l'élaboration du schéma directeur informatique 3-Absence d'une charte informatique 4- Absence d'une fiche de séparation des tâches 5- Insuffisance de personnel qualifié 6- Absence d'organisation d'ateliers de validation
	Définition d'une	5	5	25	1- Existence d'un organigramme validé par la	1- Existence d'un organigramme	1- Absence de contrôle des modifications de

Diagnostic de la démarche d'élaboration de cartographies des risques au cabinet MARISYS Sénégal

	politique inadaptée à l'organisation interne (organigramme)				<p>tutelle</p> <p>2- Existence d'un contrôle des modifications de l'organigramme</p> <p>3- Existence d'un organigramme adapté aux missions de l'entreprise</p> <p>4- Existence d'une méthode application fidèle de l'organigramme</p> <p>5- Accessibilité de l'organigramme</p>	<p>validé par la tutelle</p> <p>2- Existence d'un organigramme adapté aux missions de l'entreprise</p> <p>3- Existence d'une méthode application fidèle de l'organigramme</p>	<p>l'organigramme</p> <p>2- Mauvaise diffusion de l'organigramme</p>
2	Acquisition de ressources inappropriées	5	4	20	<p>1- Participation à des séminaires de présentation de nouvelles solutions technologiques</p> <p>2- Possibilité de procéder à des tests avant la réception définitive</p> <p>3- Existence d'une méthode rigoureuse d'élaboration des caractéristiques techniques</p> <p>4- Existence de procédures de passation des marchés</p> <p>5- Possibilité de recourir aux services d'un consultant pour mieux dimensionner nos besoins en interne</p> <p>6- Existence d'une procédure de réception des ressources informatiques</p>	<p>1- Possibilité de procéder à des tests avant la réception</p> <p>2- Participation à des séminaires de présentation de nouvelles technologies</p> <p>3- Existence de procédures de passation des marchés</p> <p>4- Possibilité de recourir à des consultants afin de mieux dimensionner nos besoins techniques en interne</p> <p>5- Existence d'une procédure de réception des ressources informatiques</p>	<p>1- Insuffisances des procédures de test et de validation des ressources</p>
	Retard dans l'acquisition	5	5	25	<p>1- Existence de ligne budgétaire pour</p>	<p>1- Existence de ligne budgétaire pour l'acquisition de ressources</p>	<p>1- Absence de protection des crédits</p>



Diagnostic de la démarche d'élaboration de cartographies des risques au cabinet MARISYS Sénégal

	des ressources informatiques				<p>l'acquisition de ressources informatiques</p> <p>2-Protection des crédits déjà alloués lors d'un réaménagement budgétaire</p> <p>3-Inscription des procédures d'acquisition de ressources informatiques dans le plan de passation de marchés (PPM)</p> <p>4- Exigence de la production d'une lettre de soumission et d'une lettre Garantie par le fournisseur désigné et la garantie du fabricant</p> <p>5- Respect des procédures de passation de marchés</p>	<p>informatiques</p> <p>2- Inscription des procédures d'acquisition de ressources informatiques dans le plan de passation de marchés (PPM)</p> <p>3- Exigence de la production d'une lettre de soumission et d'une lettre Garantie par le fournisseur désigné et la garantie du fabricant</p> <p>4- Respect des procédures de passation de marchés</p>	<p>déjà alloués lors d'un réaménagement budgétaire</p>
3	Anomalies non détectées lors du déploiement	5	3	15	<p>1- Existence de procédures de Tests de validation avant la réception définitive</p> <p>2- Possibilité de recourir à un expert pour accompagner le processus de déploiement</p> <p>3- Participation à des formations certifiantes liées rapport à la ressource</p> <p>4-Existence de certifications du fournisseur sur les ressources informatiques</p>	<p>1- Existence de certifications du fournisseur sur les ressources informatiques</p>	<p>1- Absence de procédures de tests et de validations avant la réception définitive (Partielle)</p> <p>2- Possibilité de recourir à un expert pour accompagner le processus de déploiement</p> <p>3- Absence de formations certifiantes par rapport à la ressource (Partielle)</p>

Diagnostic de la démarche d'élaboration de cartographies des risques au cabinet MARISYS Sénégal

	Retard dans le déploiement	4	4	16	<p>1- Existence d'un bon planning de déploiement</p> <p>2- Existence des prérequis au déploiement</p> <p>3- Implication des acteurs (Mail, téléphonique)</p> <p>4- Existence de l'Ordre de Service avant démarrage du déploiement</p> <p>5- Existence d'une procédure de validation technique des ressources avant de procéder au déploiement</p>	<p>1- Existence d'un bon planning de déploiement</p> <p>2- Existence des prérequis au déploiement</p> <p>3- Existence de l'Ordre de Service avant démarrage du déploiement</p>	<p>1- Non implication des acteurs (Mail, téléphonique)</p> <p>2- Absence d'une procédure de validation technique des ressources avant de procéder au déploiement (Partielle)</p>
4	Mauvaises spécifications techniques	4	4	16	<p>1- Existence de fiches de recensement des besoins auprès des acteurs</p> <p>2- Existence des termes de références</p> <p>3- Développement de la culture informatique</p> <p>4- Participation à des formations certifiantes sur les nouvelles approches technologiques</p> <p>5- Existence de cellule de veille technologique</p>	<p>1- Existence de l'élaboration des termes de références</p>	<p>1- Inexistence de fiches de recensement des besoins auprès des acteurs</p> <p>2- Développement de la culture informatique (Partiel)</p> <p>3- Participation à des formations certifiantes sur les nouvelles approches technologiques (Partielle)</p> <p>4- Absence de cellule de veille technologique</p>

Diagnostic de la démarche d'élaboration de cartographies des risques au cabinet MARISYS Sénégal

	Solution inadaptée aux besoins des utilisateurs	5	3	15	<p>1-Existence de fiche d'enquête pour le recensement des besoins avant l'acquisition ou le développement d'une solution logicielle</p> <p>2- Implication des responsables dans la phase de recette validation</p> <p>3- Existence de procédure de tests pour détecter d'éventuelles insuffisances</p> <p>4- Existence de procédures de maintenance et de suivi des mises à jour de la solution</p> <p>5- Existence de procédure de transfert de compétence de la solution acquise</p> <p>6- Existence de procédures de consultation du service informatique sur les acquisitions des ressources informatiques menées par les autres services</p>	<p>1-Existence de fiche d'enquête pour le recensement des besoins avant l'acquisition ou le développement d'une solution logicielle</p> <p>2- Existence de procédures de maintenance et de suivi des mises à jour de la solution</p> <p>3-Existence de procédure de transfert de compétence de la solution acquise</p>	<p>1- Non implication des responsables dans la phase de recette validation</p> <p>2- Absence de procédure de tests pour détecter d'éventuelles insuffisances (Partielle)</p> <p>3-absence de procédures de consultation du service informatique sur les acquisitions des ressources informatiques menées par les autres services</p>
5	Indisponibilité du système	5	5	25	<p>1- Existence de procédures de maintenance préventive des équipements de la salle machine et celle des systèmes informatiques</p> <p>2- Existence d'un groupe électrogène</p> <p>3-Existence de détecteur de variations de température</p> <p>4- Existence d'une interconnexion de secours</p> <p>5- Estimation correcte de la ligne budgétaire dédiée aux ressources téléphoniques</p> <p>6- Existence d'un onduleur central</p> <p>7- Existence de serveurs de réplication et de</p>	<p>1- Existence d'une interconnexion de secours</p> <p>2- Estimation correcte de la ligne budgétaire dédiée aux ressources téléphoniques (Partielle)</p> <p>3- Existence d'un dispositif de contrôlée d'accès des salles techniques (Partielle)</p>	<p>1- Absence de procédures de maintenance préventive des équipements de la salle machine et celle des systèmes (Partielle)</p> <p>2- Absence d'un groupe électrogène (Partielle)</p> <p>3- Absence de détecteur de variations de température</p> <p>4- Absence d'un onduleur central</p>

Diagnostic de la démarche d'élaboration de cartographies des risques au cabinet MARISYS Sénégal

					<p>sauvegarde sur un site distant</p> <p>8- Existence d'un dispositif de détection de fumée</p> <p>9- Existence d'extincteurs dans des points stratégiques</p> <p>10- Existence d'un dispositif de contrôlée d'accès des salles techniques</p> <p>11- Existence de licences logicielles originales et valides</p>		<p>5- Absence de serveurs de réplication et de sauvegarde sur un site distant</p> <p>6- Absence d'un dispositif de détection de fumée</p> <p>7- Absence d'extincteurs dans des points stratégiques</p> <p>8- Absence de licences logicielles originales et valides (Partielle)</p>
Perte de données	5	5	25	<p>1-Existence de procédures sauvegardes régulières générales et individuelles sur site et hors site</p> <p>2- Existence d'un onduleur central</p> <p>3-Existence de procédure de gestion des habilitations pour l'exploitation du système</p> <p>4- Existence des Systèmes de Protection en vigueur (pare-feu et antivirus)</p> <p>5-Existence d'un plan de reprise d'activité après incident</p>	<p>1- Existence de procédure de gestion des habilitations pour l'exploitation du système</p> <p>2- Existence des Systèmes de Protection en vigueur (pare-feu et antivirus)</p>	<p>1- Absence de procédures sauvegardes régulières générales et individuelles sur site et hors site</p> <p>2- Absence d'onduleur central</p> <p>3- Absence de plan de reprise d'activité après incident</p>	

Source : Matrice MARISYS

Tableau 11 : Echelle de cotation des risques inhérents

Score Combiné (I x P)	Ampleur du Risque Inhérent	Réponse et Traitement du Risque
15 - 25	ELEVE	Niveau de risque inacceptable– nécessité de maintenir un haut niveau de contrôle pour réduire le risque résiduel à un niveau acceptable
8-14	MOYEN	Niveau de risque inacceptable, excepté sous certaines conditions – un niveau modéré de contrôle est nécessaire pour réduire le risque résiduel à un niveau acceptable
01-7	FAIBLE	Généralement acceptable – un niveau faible de contrôle voire une absence de contrôle peut être autorisé

Source : Matrice MARISYS

- Evaluer l'exposition résiduelle.

Après avoir évalué l'efficacité du contrôle, la matrice MARISYS donne automatiquement le risque résiduel par le calcul suivant :

(Impact – Niveau de protection), (Probabilité – Niveau de Prévention).

Ainsi après que le cabinet ait évalué l'efficacité du contrôle interne il a eu automatiquement l'exposition résiduelle pour chaque risque.

Tableau 12 : Grille d'évaluation de la protection

Niveau	Qualité de la protection	Commentaire sur le CI
0	Aucune mesure de protection n'existe, ou il manque une mesure importante, ou les mesures sont inadaptées ou non mises en œuvre (protection inexistante, inadaptée et ou inefficace)	Contrôle interne clef n'offrant aucun effet protecteur (réducteur) sur l'impact du risque sur les objectifs
1	Il existe des mesures de protection moyennement ou peu adaptées et ou efficaces (protection moyennement ou peu adaptée et ou efficace)	Contrôle interne clef ayant un effet protecteur (réducteur) modéré ou moyen sur l'impact du risque
2	Il existe des mesures de protection adaptées qui sont mises en œuvre (protection adaptée et efficace)	Contrôle interne clef ayant un effet protecteur (réducteur) sur l'impact du risque
3	Il existe des mesures de protection très adaptées qui sont efficacement mises en œuvre et pour lesquelles on assure une traçabilité, un suivi et un contrôle (protection très adaptée et efficace)	Contrôle interne clef ayant un effet protecteur (réducteur) maximum sur l'impact du risque

Source : Matrice MARISYS

Tableau 13 : Grille d'évaluation de la prévention

Niveau	Qualité de la prévention	Commentaire sur le CI
0	Aucune mesure de prévention n'existe (prévention inexistante), ou il manque une mesure importante, ou les mesures sont inadaptées ou non mises en œuvre (prévention inadaptée et ou inefficace)	Qualité du contrôle interne clef très faible induisant une probabilité du risque très élevée (risque certaine) d'occurrence
1	Il existe des mesures de prévention peu ou moyennement adaptées et/ ou moyennement ou peu efficaces (prévention peu ou moyennement adaptée et ou efficace)	Qualité du contrôle interne clef moyenne induisant une probabilité du risque modérée (quasi certaine ou probable) d'occurrence
2	Il existe des mesures de prévention adaptées qui sont mises en œuvre (prévention adaptée et efficace)	Qualité du contrôle interne clef élevé induisant une probabilité du risque faible (ou peu probable) d'occurrence
3	Il existe des mesures de prévention très adaptées qui sont efficacement mises en œuvre et pour lesquelles on assure une traçabilité, un suivi et un contrôle (prévision très adaptée et efficace)	Qualité du contrôle interne clef très élevé induisant une probabilité du risque très faible (ou quasi impossible) d'occurrence

Source : Matrice MARISYS

Tableau 14 : Mesure ou évaluation des éléments du contrôle interne

Niveau	Qualité	Commentaire sur la maturité du CI (Qualité du dispositif du contrôle interne)
1	Optimisé	Les activités de contrôle sont coordonnées et la gestion des risques est conduite dans un système intégré
2	Maîtrisé ou surveillé	Les activités de contrôle sont décrites en détail et les contrôles sont effectifs. Il y a un responsable du CI et des vérifications sont faites régulièrement
3	Standardisé	Des lignes directrices ont été mises en place, les processus sont documentés et les contrôles sont adaptés
4	Informel	Les activités de contrôle internes sont mises en place mais sans standardisation. Ils dépendent des individus
5	Non ou peu fiable	Peu ou pas d'activités de contrôle interne sont mises en place. L'organisation est à risque

Source : Matrice MARISYS

Tableau 15 : Echelle de mesure du risque résiduel

Score Combiné (I x P)	Ampleur du Risque Résiduel	Réponse et traitement du risque
15 - 25	ELEVE	Niveau de risque résiduel inacceptable- les contrôles sont inadéquats (mauvais design) ou inefficaces (mauvaise application). Contrôles nécessitent refonte complète ou efforts significatifs dans leur application. Le risque est soit Traité, Transféré ou terminé.
8-14	MOYEN	Niveau de risque résiduel inacceptable- les contrôles sont inadéquats (mauvais design) ou inefficaces (mauvaise application). Contrôles nécessitent plus d'efforts dans leur application. Le risque est soit Traité, Transféré ou terminé.
01-7	FAIBLE	Risque résiduel généralement acceptable – requiert une amélioration minimale des contrôles, ou maintien en l'état. Le risque peut être toléré.

Source : Matrice MARISYS

- Identifier l'appétence au risque du management (niveau : Traiter, Tolérer, Transférer ou Terminer).

Après avoir déterminé le risque résiduelle les managers des différents départements ont la possibilité de choisir parmi les réponses proposées par la matrice MARISYS à savoir : Traiter, Tolérer, Transférer. Ainsi dans notre cas cela a été appliqué par l'exemple des managers de la DSI.

- Déterminer le niveau de priorisation (échelle de 1 à 3) et classement du risque (déjà survenu : (Oui/Non).

Après avoir déterminé le niveau d'appétence les managers ont la possibilité de choisir un niveau de priorisation à l'aide de 1 à 3 après avoir précisé si le risque a été déjà survenu OUI ou non et cela à l'aide du tableau suivant.

- Proposer un plan de mitigation (recommandations, responsables, période).

Cette section permet avec l'ensemble des managers de proposer des recommandations en fonction des faiblesses identifiées.

Tableau 16 : Evaluation du contrôle interne, risque résiduel et recommandations

Réf	Risques retenus	Evaluation de la maturité du contrôle interne			Risques Résiduels			Appétence pour le risque	Déjà survenu (OUI/NON)	Actions (Recommandations)
		Protection (pro) 0 à 3	Prévention (Pré) 0 à 3	Niveau de maturité du CI (1 à 5)	Impact = I-Pro	Probabilité = P-Pré	Score = P×I			
1	Définition d'une politique inadaptée aux missions de l'entreprise	0	1	1	5	3	15	Traiter	OUI	1- Mettre en place un schéma directeur informatique 2- Elaborer des fiches d'interviews et d'expression des besoins pour l'élaboration du schéma directeur informatique permettant d'impliquer tous les acteurs dans la définition de la politique 3- Rédiger une charte informatique et faire signer par l'ensemble des acteurs 4- Elaborer une fiche de séparation des tâches au sein du personnel de l'entreprise 5- Recruter un ingénieur en réseau et maintenance pour pourvoir au poste de Chef de la division réseau et



**Diagnostic de la démarche d'élaboration de cartographies des risques au cabinet MARISYS Sénégal**

										<p>maintenance</p> <p>6- Prévoir la tenue d'atelier de validation de la politique informatique</p>
	Définition d'une politique inadaptée à l'organisation interne (organigramme)	1	1	1	4	4	16	Traiter	OUI	<p>1- Contrôler les modifications de l'organigramme</p> <p>2- Diffuser l'organigramme et ses mises à jour éventuelles auprès de l'ensemble des agents</p>
2	Acquisition de ressources inappropriées	1	2	3	4	2	8	Traiter	OUI	1- Mettre en place des procédures rigoureuses de test et de validation des ressources informatiques
	Retard dans l'acquisition des ressources informatiques	1	2	3	4	3	12	Traiter	OUI	1- Protéger les crédits déjà alloués aux ressources informatiques lors d'un réaménagement budgétaire
3	Anomalies non détectées lors du déploiement	1	0	2	4	3	12	Traiter	OUI	<p>1- Mettre en place des procédures de tests et de validations avant la réception définitive</p> <p>2- Recourir à un expert pour accompagner le processus de</p>

Diagnostic de la démarche d'élaboration de cartographies des risques au cabinet MARISYS Sénégal

										déploiement  3- Participer à des formations certifiantes sur la ressource à déployer
	Retard dans le déploiement	1	1	3	3	3	9	Traiter	OUI	1- Elaborer des fiches de sensibilisation des acteurs au déploiement des ressources  2- Renforcer la procédure de validation technique des ressources informatiques à déployer
4	Mauvaises spécifications techniques	0	1	2	4	3	12	Traiter	OUI	1- Mettre en place des fiches de recensement des besoins auprès des acteurs  2-Développer la culture informatique des acteurs  3- Participer à des séances de formations certifiantes  4- Mettre en place une cellule de veille technologique

**Diagnostic de la démarche d'élaboration de cartographies des risques au cabinet MARISYS Sénégal**

	Solution inadaptée aux besoins des utilisateurs	1	1	3	4	2	8	Traiter	OUI	<p>1- Associer les responsables dans la phase de recette validation</p> <p>2- Mettre en place des procédures de tests pour détecter d'éventuelles insuffisances</p> <p>3- Mettre en place des procédures de consultation du service informatique sur les acquisitions de ressources informatiques par les autres services</p>
5	Indisponibilité du système	1	1	2	4	4	16	Traiter	OUI	<p>1- Elaborer et signer un contrat de maintenance de l'ensemble des équipements informatiques</p> <p>2- Installer un groupe électrogène exclusivement dédié à l'entreprise pour assurer le relais automatique après délestages/dysfonctionnements du courant de la SENELEC</p> <p>3- Acquérir et installer un détecteur de variations de température disposant de fonctionnalités d'alertes par sms et par messagerie électronique</p> <p>4- Acquérir et installer des onduleurs centraux dans les salles techniques pour sauvegarder la distribution électrique avant le déclenchement du</p>

Diagnostic de la démarche d'élaboration de cartographies des risques au cabinet MARISYS Sénégal

										<p>groupe électrogène</p> <p>5- Acquérir et déployer des dispositifs (Serveurs, Cloud, etc.) de sauvegarde et de réplication sur sites distants</p> <p>6- Acquérir et installer un détecteur de fumée/d'incendie avec des fonctionnalités d'alerte sonore, de sms et de messagerie électronique</p> <p>7- Acquérir et fixer des extincteurs dans les zones stratégiques de l'entreprise</p> <p>8- Généraliser l'acquisition de licences logicielles valides</p>
	Perte de données	1	2	3	4	3	12	Traiter	OUI	<p>1- Mettre en place des procédures sauvegardes régulières générales et individuelles sur site et hors site</p> <p>2- Acquérir et installé un onduleur central</p> <p>3-Mettre en place un plan de reprise d'activités après incident</p>

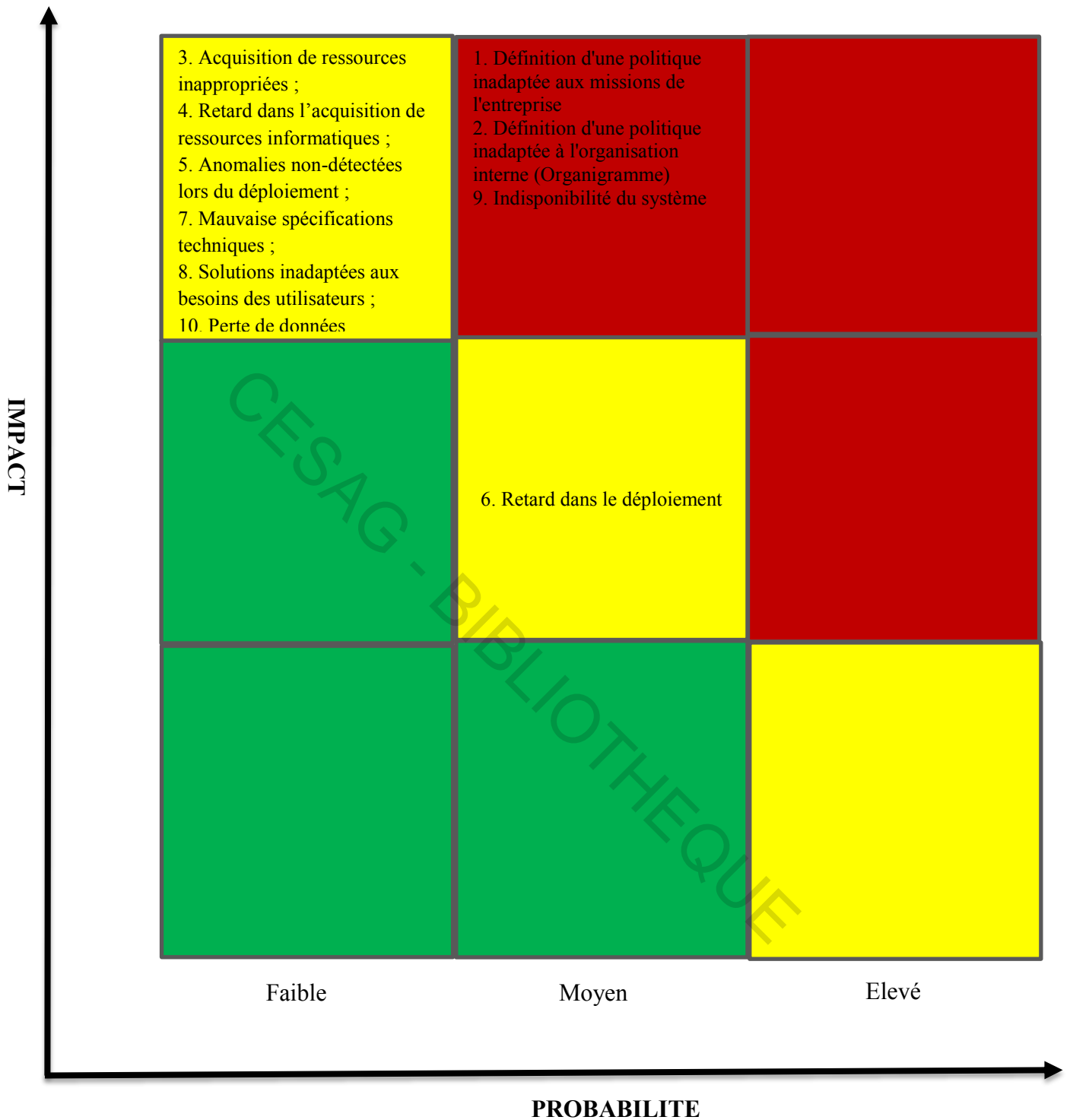
Source Matrice MARISYS

- Proposer, le cas échéant une mission d'audit (audit proposé, type, objectif, effort indicatif).

## 5.2. Présentation de la matrice

Dans cette partie nous présenterons la matrice des risques de notre exemple qui est une représentation graphique de l'évaluation des risques et le tableau des recommandations. Cette représentation graphique nous donne une image fidèle du niveau de risques avec prise en compte de probabilité et d'impact. Ces risques seront classés en trois (3) catégories à l'aide de notre échelle de cotation de risque.

CESAG - BIBLIOTHEQUE



Source Matrice MARISYS

La cartographie des risques de la direction du système d'information met en exergue trois niveaux de criticité des risques délimités par les couleurs : rouge, jaune, verte.

La zone avec la coloration verte des risques à criticité faible. Pour c'est zone on n'a pas besoin de mesure d'urgence, on peut ne pas prendre des mesures car pour ce genre de risques le dispositif du contrôle interne en place assure leur maîtrise.

La zone avec la coloration jaune des risques à criticité moyenne. Pour ces risques la direction doit juger si elle doit renforcer le dispositif de contrôle interne ou non pour éviter leur aggravation car quand bien même ayant une criticité moyenne leur impact sur les processus n'est pas souvent négligeable.

La zone avec la coloration rouge des risques à criticité élevée. Pour c'est zone on a besoin de mesure d'urgence, pour ces risques on doit faire des traitements particuliers et les suivre jusqu'à un niveau acceptable en effet l'impact de ces risques sur les processus n'est pas négligeable et peut causer d'énorme dégâts.

Pour ramener ces risques à un niveau acceptable le cabinet MARISYS va faire des propositions d'actions à la direction du système d'information et des recommandations.

### **5.3. Plans d'actions et recommandations**

La cartographie des risques de la direction du système d'information étant établi, le cabinet MARISYS proposera ici des mesures pour ramener chaque risque de leurs niveaux actuels à un niveau acceptable.

Pour ce faire le cabinet MARISYS propose dans un premier temps un plan d'actions et dans un second des recommandations.

#### **5.3.1 Plan d'actions**

Après la cartographie de la direction du système d'information le cabinet MARISYS a fait une proposition de plan d'actions à la direction du système d'information présentée dans le tableau suivant :

Tableau 17 : Proposition du plan d'actions

Risques	Actions	Périodes retenues pour la mise en œuvre		Responsables de l'action	Coûts estimatifs
		Début	Fin		
1. Définition d'une politique inadaptée aux missions de l'entreprise	Mettre en place un schéma directeur informatique	Sept-17	Oct-17	DSI	30 millions
2. Définition d'une politique inadaptée à l'organisation	Diffuser l'organigramme et ses mises à jour éventuelles auprès de l'ensemble des agents	Sept-17	Permanent	RH	Aucun
9. Indisponibilité du système	Acquérir et déployer des dispositifs (Serveurs, Cloud, etc.) de sauvegarde et de réplique sur sites distants	Janv-18	Avr-18	DSI	A évaluer
3. Acquisition de ressources inappropriées	Mettre en place des procédures rigoureuses de test et de validation des ressources informatiques	Nov-17	Janv-18	DSI	Aucun
4. Retard dans l'acquisition de ressources informatiques ;	Protéger les crédits déjà alloués aux ressources informatiques lors d'un réaménagement budgétaire	Févr-18	Permanent	DAF	Aucun
5. Anomalies non-détectées lors du déploiement	Mettre en place des procédures de tests et de validations avant la réception définitive	Janv-18	Févr-18	DSI	Aucun
7. Mauvaise spécifications techniques	Mettre en place des fiches de recensement des besoins auprès des acteurs	Nov-17	Déc-17	DSI	Aucun
8. Solutions inadaptées aux besoins des utilisateurs	Associer les responsables dans la phase de recettes validation	Sept-17	Permanent	DSI	Aucun
10. Perte de données	Mettre en place des procédures de sauvegardes régulières générales et individuelles sur site et hors site	Oct-17	Nov-17	DSI	A évaluer
6. Retard dans le déploiement	Renforcer la procédure de validation technique des ressources informatiques à déployer	Déc-17	Permanent	DSI	A évaluer

Source Matrice MARISYS



### 5.3.2 Recommandations

Après la revue du dispositif du contrôle interne de la direction du système d'information de l'entreprise test le cabinet MARISYS procède à la formulation des recommandations pour les différents risques.

➤ **Recommandations relatives à la définition d'une politique inadaptée aux missions de l'entreprise**

La direction du système d'information pour mettre en place une politique adaptée aux missions de l'entreprise, doit se doter d'un schéma directeur informatique, élaborer des fiches d'interviews et d'expression des besoins pour l'élaboration du schéma directeur informatique afin d'impliquer tous les acteurs dans la définition de la politique informatique. Elle doit rédiger une charte informatique et faire signer par l'ensemble des acteurs et prévoir la tenue d'atelier de validation de la politique informatique.

➤ **Recommandations relatives à la définition d'une politique inadaptée à l'organisation interne (organigramme)**

Pour avoir une politique informatique en cohérence avec l'organigramme de l'entreprise, la direction générale doit contrôler les modifications de l'organigramme et s'assurer de diffusion de l'organigramme et ses mises à jour éventuelles auprès de l'ensemble des agents de l'entreprise.

➤ **Recommandations relatives à l'indisponibilité du système**

Pour lutter contre l'indisponibilité du système, la direction du système d'information doit élaborer et signer un contrat de maintenance de l'ensemble des équipements informatiques, installer un groupe électrogène exclusivement dédié à l'entreprise pour assurer le relais automatique après délestages ou dysfonctionnements du courant de la SENELEC, acquérir et installer un détecteur de variations de température disposant de fonctionnalités d'alertes par sms et par messagerie électronique, acquérir et installer des onduleurs centraux dans les salles techniques pour sauvegarder la distribution électrique avant le déclenchement du groupe électrogène, acquérir et déployer des dispositifs (Serveurs, Cloud, etc.) de sauvegarde et de réplication sur sites distants, acquérir et installer un détecteur de fumée/d'incendie avec des fonctionnalités d'alerte sonore, de sms et de messagerie électronique, acquérir et fixer des extincteurs dans les zones stratégiques de l'entreprise, généraliser l'acquisition de licences logicielles valides.

➤ **Recommandation relative aux retards dans l'acquisition des ressources informatiques**

Pour faire face aux retards dans l'acquisition des ressources informatiques du réaménagement budgétaire la direction administrative et financière doit protéger les crédits déjà alloués aux ressources informatiques lors d'un réaménagement budgétaire.

➤ **Recommandations relatives aux anomalies non-détectées lors du déploiement**

Pour faire face aux anomalies non-détectées, la direction du système d'information doit mettre en place des procédures de tests et de validations avant la réception définitive, recourir à un expert pour accompagner le processus de déploiement, participer à des formations certifiantes ou non certifiantes sur la ressource à déployer.

➤ **Recommandations relatives aux mauvaises spécifications techniques**

Pour avoir des bonnes spécifications techniques, la direction du système d'information doit mettre en place des fiches de recensement des besoins auprès des acteurs, développer la culture informatique des acteurs, participer à des séances de formations certifiantes, mettre en place une cellule de veille technologique.

➤ **Recommandations relatives aux pertes de données**

Pour réduire les pertes de données, la direction du système d'information doit mettre en place des procédures sauvegardes régulières générales et individuelles sur site et hors site, acquérir et installé un onduleur central, mettre en place un plan de reprise d'activités après incident.

➤ **Recommandations relatives aux Retards dans le déploiement des ressources informatiques**

Pour réduire les retards lors des déploiements des ressources informatiques, la direction du système d'information doit renforcer la procédure de validation technique des ressources informatiques à déployer, élaborer des fiches de sensibilisation des acteurs au déploiement des ressources.

➤ **Recommandation relative à l'acquisition de ressources inappropriées**

Pour une bonne acquisition des ressources, la direction du système d'information doit mettre en place des procédures rigoureuses de test et de validation des ressources informatiques.

➤ **Recommandations relatives aux solutions inadaptées aux besoins des utilisateurs**

Pour réduire le nombre de solutions inadaptées aux besoins des utilisateurs, la direction du système d'information doit associer les responsables dans la phase de recette validation, mettre en place des procédures de tests pour détecter d'éventuelles insuffisances, mettre en place des procédures de consultation du service informatique sur les acquisitions de ressources informatiques par les autres services.

## **Conclusion**

Ce chapitre nous a permis de décrire la démarche du cabinet MARISYS pour l'élaboration d'une cartographie des risques, celle-ci étant développée dans le but de répondre aux besoins des entreprises pour la gestion des risques auxquels elles sont exposées. Cependant elle se doit d'être une démarche performante pour répondre aux soucis des entreprises, ainsi dans le chapitre six (6) il sera question pour nous de diagnostiquer cette démarche par l'analyse de ses forces et ses faiblesses et terminer par des recommandations.

## CHAPITRE 6 : DIAGNOSTIC DE LA DEMARCHE D'ELABORATION D'UNE CARTOGRAPHIE DES RISQUES

Notre description de la démarche du cabinet MARISYS pour l'élaboration d'une cartographie des risques nous a permis de mieux cerner les aspects caractéristiques de cette démarche, afin de faire une analyse de ses forces et faiblesses. Ainsi dans ce chapitre nous aborderons les forces et faiblesses de la démarche et nous terminerons par quelques recommandations dans le but de permettre au cabinet MARISYS d'améliorer sa démarche.

### 6.1. Forces et faiblesses de la démarche du cabinet MARISYS

Toute œuvre humaine ayant des imperfections, dans cette partie nous ferons ressortir de fond en comble les différentes forces et faiblesses de la démarche à travers ses différentes étapes.

#### 6.1.1. Les forces de la démarche du cabinet MARISYS

Après analyse de la démarche du cabinet pour la cartographie des risques, il ressort que cette démarche comporte un ensemble de bonnes pratiques susceptibles de produire une cartographie des risques fiables.

Notre diagnostic nous a permis de relever les forces suivantes :

##### ➤ Vue générale

- la démarche est adaptée à l'environnement et à la réalité des entreprises publiques et privées, cela s'explique par la diversité des entreprises-clients du cabinet ;
- elle est inspirée des meilleures pratiques et approches en matière de gestion des risques comme le COSO 1 et COSO 2. En effet, dans le manuel de guide du cabinet, il a été constaté que la grande partie de ses étapes d'élaboration de cartographies sont inspirées du COSO ;
- après comparaison, il ressort que cette démarche est en adéquation avec les autres approches d'élaboration d'une cartographie des risques des entreprises ;
- la démarche intègre une étape de formation du client du cabinet sur les concepts clés de la cartographie des risques. Ladite étape s'étale sur une durée de trois (03) jours et au-delà, en fonction du niveau de compréhension du client ;
- la démarche est simple et pratique.

➤ **Périmètre couvert**

- la démarche couvre tous les départements de l'entreprise-cliente du cabinet dans l'élaboration de la cartographie des risques ;
- la démarche peut s'adapter à toutes activités et entreprises quel que soit la taille, la forme et le poids économique ;
- la démarche peut permettre d'élaborer la cartographie de tous les secteurs d'activités car elle n'est pas restrictive.

➤ **Les différentes étapes**

- la démarche respecte les différentes étapes spécifiques et générales d'un processus d'élaboration de cartographies des risques ;
- il existe un enchaînement logique entre les différentes étapes et phases de la démarche ;
- les différentes étapes de la démarche sont en adéquation avec la segmentation des activités ;
- les étapes générales de la démarche sont formalisées à travers le manuel d'application du cabinet.

➤ **Acteurs**

- la démarche étant participative elle facilite une implication de tous les acteurs. Ainsi toute l'entreprise se sent concernée par la maîtrise des risques ;
- la démarche permet une réelle communication entre les différents acteurs de l'entreprise en matière de gestion des risques car force est de constater qu'il n'y a souvent pas de réelle communication entre certains départements de l'entreprise-cliente avant le démarrage de la mission du cabinet ;
- la démarche permet aux acteurs d'être fortement impliqués dans la gestion du risque du fait que chaque acteur est responsable du risque engendré par ses activités ;
- la démarche donne la chance à tous les acteurs de l'entreprise de s'exprimer quel que soit leur niveau de responsabilité ainsi elle permet de prendre en compte tous les risques au niveau de l'entreprise ;
- une discussion pour l'amélioration de la démarche est tenue chaque année par l'ensemble des acteurs responsables de cette démarche qui sont des consultants avec plusieurs années d'expériences dans le domaine du management des risques.

➤ **Cartographie par l'approche des processus**

- la démarche s'inspire des approches top down et bottom up, ce qui lui permet de pouvoir identifier complètement et clairement les différents processus ;
- l'utilisation des fiches de postes permet l'identification détaillée des processus et activités.

➤ **Identification et analyses des risques inhérents**

- une identification des risques basée sur l'atteinte des objectifs, ainsi après analyse des processus et activités de l'entreprise, il ne ressort que ce qui pourrait impacter les objectifs ;
- la démarche d'identification est basée sur les check-lists ce qui permet d'énumérer un certain nombre de risques éventuels auxquels l'entreprise pourrait être exposé ;
- l'identification par analyse des activités : décomposition des processus en activités identification des risques associés (conséquences potentielles de la non/mauvaise exécution des tâches) ;
- l'identification par l'analyse des faits historique en recherchant les risques qui ont menacé l'entreprise dans le passé ;
- la démarche propose une base de données des risques génériques ce qui permet une identification facile des risques de certains processus génériques ;
- une identification basée sur l'analyse de l'environnement (menaces de l'environnement économique, technologique) ;
- une identification des risques basée souvent sur le recours à des experts de certains domaines d'activités ;
- une identification des risques faite selon l'approche intuitive ;
- la démarche fournit un ensemble de typologie de risque inspiré de la typologie générale des risques reconnue par les bonnes pratiques en matière de gestion de risque.

➤ **Evaluation des risques inhérents**

- la démarche d'évaluation des risques inhérents est convaincante, en effet elle est basée sur une analyse des critères quantitatives et qualitatives de l'impact et de la probabilité ;
- une énumération des causes et conséquences des risques afin de mieux voir les conséquences de ces risques et donc de mieux évaluer leur impact de souvenance

- la démarche a une définition formelle de l'échelle d'évaluation des impacts et probabilités des risques ;
- une cotation de la criticité du risque inhérent commune à la généralité des bonnes pratiques (Probabilité  $\times$  Impact) ;
- l'existence d'une échelle de cotation du risque inhérent, ce qui permet de définir le niveau de priorité du risque en fonction des trois couleurs (rouge, jaune, vert).

➤ **Identifications et évaluation du contrôle interne**

- la démarche identifie les éléments clés du contrôles interne existants (forces apparentes) et inexistantes (faiblesses apparentes) pour chaque risque ;
- une définition de la typologie de chaque contrôle identifié (préventif, protectif, détectif) ;
- une identification des contrôles faite après des entretiens et des tests de permanences et de conformités ;
- existence d'une échelle pour l'évaluation du contrôle interne ;
- la notion de contrôle formel et informel est prise en compte dans l'évaluation du contrôle interne, en effet le cabinet vérifie si le contrôle interne mis en place par l'entreprise-cliente pour chaque risque est formel ou informel, afin d'émettre des recommandations pour formaliser le contrôle informel.

➤ **Evaluation des risques résiduels**

- une cotation de la criticité des risques résiduels faite dans la même logique que celle des risques inhérents (Probabilité résiduelle  $\times$  Impact résiduel) ;
- une évaluation automatique du risque résiduel après évaluation du contrôle interne, en effet l'outil d'élaboration de cartographies du cabinet donne automatiquement la cotation du risque résiduel après évaluation du contrôle interne ;
- l'existence d'une échelle de cotation du risque résiduel qui permet de mettre en exergue le niveau de priorité de résolution du risque résiduel en fonction des trois couleurs (rouge, jaune, vert) ;
- la prise en compte du seuil de tolérance dans l'évaluation du risque, en effet le cabinet définit le seuil de tolérance par la couleur verte de l'échelle d'évaluation du risque résiduel.

➤ **Plans d'action**

- la démarche permet de ramener le niveau des risques résiduels à un niveau raisonnable grâce à une définition de plans d'actions ;
- la démarche permet la nomination d'un responsable pour le suivi de chaque plan d'action, dans la mesure où le cabinet pour chaque plan d'action responsabilise un personnel de l'entreprise-cliente ;
- la démarche prend en compte la notion de chronogramme d'exécution des recommandations, puisqu'elle définit d'un calendrier d'exécution des plans d'action ;
- la démarche permet de définir des indicateurs pour le suivi de la recommandation ;
- la démarche prend en compte les coûts approximatifs de mise en œuvre des différents plans d'actions.

➤ **Actualisation**

- la démarche permet une mise à jour facile de la matrice avec une insertion facile de nouveaux risques pour analyse.

➤ **Matrice des risques**

- l'existence d'une matrice qui découpe les zones des risques en trois couleurs (rouge, jaune, vert);
- la démarche est progressive, car l'insertion de nouveaux risques impacte automatiquement la matrice ce qui permet une mise à jour de celle-ci ;
- l'existence d'une matrice consolidée des risques.

### **6.1.2. Faiblesses de la démarche du cabinet MARISYS**

Nous remarquons quelques faiblesses notoires qui pourraient être préjudiciables à la démarche du cabinet.

Ces faiblesses seront énumérées selon les volets suivants :

➤ **Vue générale**

- l'outil d'élaboration de la cartographie des risques du cabinet est fait à partir du logiciel Excel ce qui ne garantit pas la sécurité des données d'une entreprise lorsque celles-ci sont confidentielles ou sensibles.



➤ **Identification et analyses des risques inhérents**

- la sélection de trois (03) risques jugés majeurs n'est pas toujours fiable car le choix peut être subjectif ;
- il n'y a pas une définition donnée pour les types de risques ce qui provoque une incompréhension quant au choix du type de risque.

➤ **Identification et évaluation du contrôle interne**

- une évaluation du contrôle interne sans un questionnaire de contrôle interne formalisé ;

## 6.2. Recommandations

La démarche du cabinet MARISYS Sénégal pour l'élaboration d'une cartographie des risques est énormément efficace et facile à adopter. Néanmoins, nous pouvons proposer quelques améliorations qui pourront permettre de faire face aux faiblesses que nous avons identifiées.

➤ **Vue générale**

- nous suggérons l'utilisation d'un logiciel plus performant qu'Excel pour faciliter et augmenter la qualité et le temps de la conception des cartographies et la sécurité des données (développer un logiciel avec un langage de programmation JAVA EE).

➤ **Acteurs**

- afin d'avoir une bonne évaluation des risques des entreprises-clientes nous proposons au cabinet de s'assurer que les acteurs responsables de l'évaluation des risques dans ces entreprises aient une bonne compréhension du concept de risque et soient réellement impliqués dans l'élaboration de leur cartographie des risques.

➤ **Identification et analyses des risques inhérents**

- en ce qui concerne la fixation à trois (03) des risques à traiter il serait peut-être plus judicieux de ne pas limiter le nombre à trois (03) mais plutôt de les traiter en fonction du nombre qui serait convenable à la gestion des risques d'un processus, d'un sous processus, d'une activité ;
- pour la typologie des risques nous suggérons une illustration de chaque typologie de risque afin de mieux faire correspondre chaque risque à sa typologie.

➤ **Evaluation des risques inhérents**

- en ce qui concerne l'évaluation des risques par les propriétaires du risque, chose que nous trouvons bien comme approche, il faudrait cependant s'assurer que les propriétaires de ces risques aient de l'expérience pour évaluer leurs risques afin d'avoir une bonne notation des risques ;
- nous proposons pour l'échelle d'évaluation des risques un découpage en quatre (04) zones au lieu de trois (03) pour une meilleure évaluation des risques inhérents.

➤ **Identification et évaluation du contrôle interne**

- pour l'évaluation du contrôle interne nous recommandons l'utilisation de questionnaire de contrôle interne afin d'avoir pour chacun des points de contrôle, un jugement critique et une observation plus complète.

➤ **Evaluation des risques résiduels**

- nous proposons pour l'échelle d'évaluation des risques un découpage en quatre zones (04) au lieu de trois (03) pour une meilleure évaluation des risques résiduels.

➤ **Matrice des risques**

- nous proposons un découpage de la matrice en quatre zones de niveau du risque pour permettre une bonne vision à prendre en compte dans la même logique de l'évaluation des risques résiduels.

## Conclusion

Ce chapitre nous a permis de faire ressortir les forces et les faiblesses de la démarche du cabinet MARISYS dans l'élaboration de la cartographie des risques et de faire des recommandations dans le but de contribuer à l'amélioration de cette démarche. Nous n'avons pas eu faire plusieurs recommandations et cela du fait de la pertinence et de l'efficacité de la démarche du cabinet MARISYS pour l'élaboration d'une cartographie des risques.

## CONCLUSION DE LA DEUXIEME PARTIE

La deuxième partie de notre mémoire, nous a permis de faire un diagnostic de la démarche du cabinet MARISYS pour l'élaboration d'une cartographie des risques, après une prise de connaissance du cabinet, une description de sa démarche et une application pratique de celle-ci à un cas parmi les clients du cabinet dont nous nous sommes réservés de taire le nom pour des raisons de confidentialité.

Ce diagnostic nous a fait ressortir les forces et les faiblesses de la démarche, les faiblesses pour lesquelles nous avons fait des recommandations pour une amélioration de cette démarche afin d'aboutir à un management de risques encore plus efficace.

CESAG - BIBLIOTHEQUE

## CONCLUSION GENERALE

Les entreprises sont de plus en plus sujettes à des risques de tout type dans leur gestion quotidienne des affaires. La gestion des risques devient alors un sujet important dans la vie de toute entreprise. Elle doit cependant aider l'entreprise dans l'atteinte de ses objectifs et la protection de ses actifs.

La cartographie des risques, se présentant comme un outil indispensable pour l'entreprise dans la gestion des risques, devient donc un préalable en matière de protection des actifs des entreprises.

L'objectif principal de notre étude était de diagnostiquer la démarche du cabinet MARISYS pour l'élaboration de cartographies des risques.

Notre travail nous a permis, de diagnostiquer la démarche du cabinet pour l'élaboration de cartographies des risques à travers les différentes phases et étapes. Ce qui nous a permis de ressortir les forces et faiblesses de cette démarche.

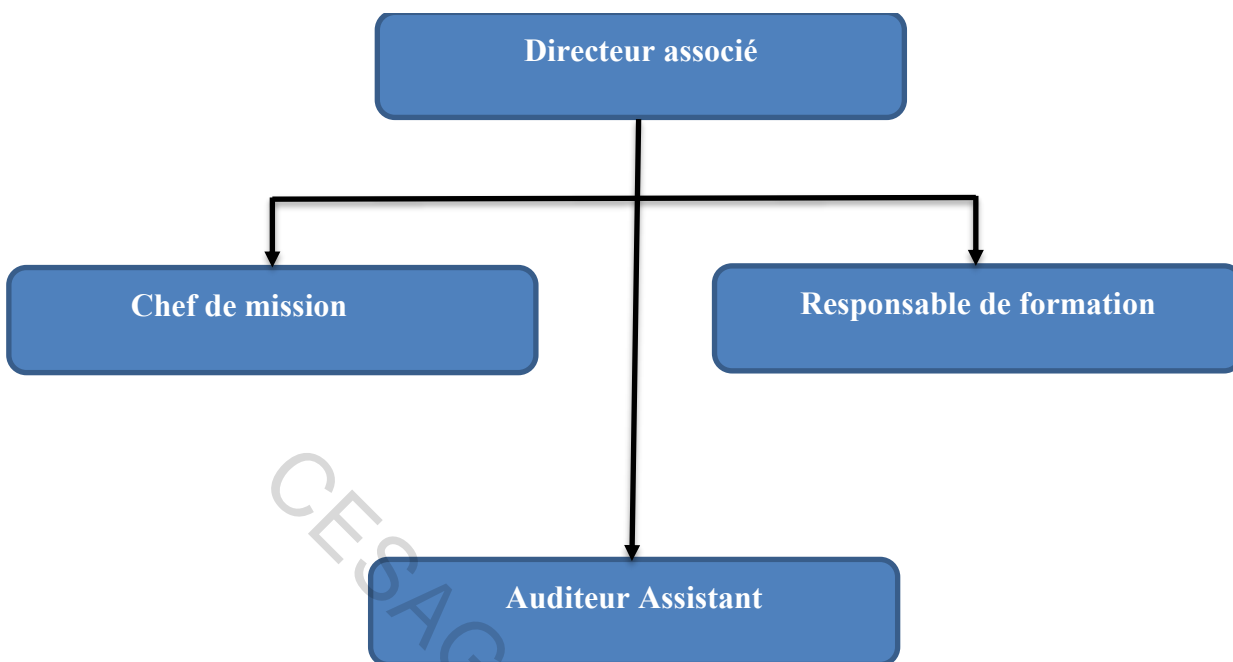
Nous avons pour finir proposer des recommandations au cabinet pour l'amélioration de la démarche. Nous n'avons pas eu à proposer beaucoup de recommandations, du fait de la pertinence et de l'efficacité de cette démarche.

Au terme de notre travail, nous pouvons affirmer que la démarche du cabinet MARISYS est pertinente et efficace pour l'élaboration de cartographies des risques. Par ailleurs, nous pensons avoir contribué à l'amélioration de cette démarche du cabinet pour l'élaboration d'une cartographie des risques et nous espérons fortement que notre travail puisse aider les lecteurs dans la compréhension de la démarche du cabinet MARISYS pour l'élaboration d'une cartographie des risques.

**ANNEXES**

CESAG - BIBLIOTHEQUE

Annexe 1 : Organigramme du Cabinet MARISYS Sénégal du 12/01/2018



Annexe 2 : Matrice MARISYS

Ref.	Mission/Objectifs/ Activités	Risques retenus	Type de risque	Causes probables	Conséquences probables	Entités impliquées (Propriétaire, Fournisseur, Client, Appui)	Risque Inhérent			Bonnes pratiques de CI de maîtrise des risques	Éléments clés du Contrôle interne existants et inexistant	
							Impact (I) 1 à 5	Probabilité (P) 1 à 5	Score = P x I		Existants (forces apparentes)	Inexistants (faiblesses apparentes)
	Définition d'une politique inadaptée aux missions de l'entreprise		Risque Stratégique	1- Absence de visibilité des missions de l'entreprise 2- Manque d'expérience 3- Manque de budget ou Prévision erronée 4- Insuffisance ou manque de compétence des ressources humaines 5- Absence de recensement des besoins 6- Faible implication des agents	1- Mauvaise Orientation stratégique 2- Incompréhension de la mission 3- Pilotage à vu ou surcharge de travail 4- Perte financière 5- Perte de temps 6- Atteinte de l'image	DSI ET TOUS LES SERVICES DE L'ENTREPRISE	5	4	20	1- Existence d'un schéma directeur informatique 2- Existence d'une fiche d'interviews et d'expression des besoins pour l'élaboration du schéma directeur informatique 3- Existence d'une charte informatique et signée 4- Existence d'une fiche de séparation des tâches 5- Possibilité de recourir aux services d'un consultant 6- Existence de personnel qualifié suffisant 7- Organisation d'ateliers de validation 8- Existence d'un plan d'actions 9- Validation des documents par le conseil de surveillance	1- Possibilité de recourir aux services d'un consultant 2- Existence d'un plan d'actions 3- Validation des documents par le conseil de surveillance	1- Absence d'un schéma directeur informatique 2- Inexistence d'une fiche d'interviews et d'expression des besoins pour l'élaboration du schéma directeur informatique 3- Absence d'une charte informatique 4- Absence d'une fiche de séparation des tâches 5- Insuffisance de personnel qualifié 6- Absence d'organisation d'ateliers de validation
	Définir la politique			1- Manque de Budget pour la définition de la politique informatique 2- Absence de réunion de cadrage (Lancement)	1- Pilotage à vue 2- Investissements informatiques non maîtrisés 3- Inefficacité des services					1- Existence d'un budget pour la politique informatique de l'Agence 2- Tenue d'une réunion de cadrage	1- 2- 3- 4- 5-	1- Absence de budget pour la définition de la politique informatique 2- Absence de réunion de cadrage 3- Absence d'une bonne

Diagnostic de la démarche d'élaboration de cartographies des risques au cabinet MARISYS Sénégal

Ref.	Mission/Objectifs/ Activités	Risques retenus	Type de risque	Causes probables	Conséquences probables	Entités impliquées (Propriétaire, Fournisseur, Client, Appui)	Évaluation de la maturité du contrôle interne			Risque résiduel			Appétence pour le risque	Classement	
							Protection (Pro) 0 à 3	Prévention (Pré) 0 à 3	Niveau de maturité CI 1 à 5	Impact = I - Pro	Probabilité = P - Pré	Score = P x I		Déjà Surveillé Oui/Non	Rang de priorité Échelle 1 à 3
			Risque Stratégique	1- Absence de visibilité des missions de l'entreprise 2- Manque d'expérience 3- Manque de budget ou Prévision erronée 4-Insuffisance ou manque de compétence des ressources humaines 5- Absence de recensement des besoins 6- Faible implication des agents	1- Mauvaise Orientation stratégique 2- Incompréhension de la mission 3- Pilotage à vu ou surcharge de travail 4- Perte financière 5- Perte de temps 6- Atteinte de l'image	DSI ET TOUS LES SERVICES DE L'ENTREPRISE	0	1	1	5	3	15	Traiter	Oui	1- Zone d'audit et de traitement des risques prioritaires (Action immédiate)
	Définir la politique			1- Manque de Budget pour la définition de la politique informatique 2- Absence de réunion de	1- Pilotage à vue 2- Investissements informatiques non maîtrisés										1- Zone d'audit et de traitement des risques



## Diagnostic de la démarche d'élaboration de cartographies des risques au cabinet MARISYS Sénégal

Ref.	Mission/Objectifs/ Activités	Risques retenus	Type de risque	Appétence pour le risque	Classement		Plan de management des risques					
					Déjà Surveillé Oui/Non	Rang de priorité Échelle 1 à 3	Actions (Recommandations)	Période retenue pour mise en œuvre		Responsable de l'action	Coût estimatif	Indicateur de suivi
								Début	Fin			
			Risque Stratégique				1- Zone d'audit et de traitement des risques prioritaires (Action immédiate)	1- Sep2017	1- Oct 2017	1- DSI	1- 30 Millions	1- SDI mis en place et appliqué
	Définition d'une politique inadaptée aux missions de l'entreprise			Traiter	Oui		2- Elaborer des fiches d'interviews et d'expression des besoins pour l'élaboration du schéma directeur informatique permettant d'impliquer tous les acteurs dans la définition de la politique	2- Oct2017	2- nov2017	2- DSI	2- 10Millions	2- Fiche d'interviews élaboré et nombre de personne interviewé
							3- Rédiger une charte informatique et faire signer par l'ensemble des acteurs	3- Nov 2017	3- Dec 2017	3- DSI	3- Aucun	3-Charte informatique redigée et signée
							4- Elaborer une fiche de séparation des tâches au sein du personnel	4- Nov 2017	4- Déc 2017	4- DSI-DF	4- aucun	4- Fiche de séparation des tâches élaborée
							5- Recruter un ingénieur en réseau et maintenance pour pourvoir au poste de Chef de la division réseau et maintenance	5- Nov 2017	5- Déc 2017	5- DSI	5- 1Million	5- Nombre d'ingénieur recruté
							6- Prévoir la tenue d'atelier de	6- Déc 2017	6- Déc 2017	6- DSI		6- Nombre d'atelier de validation tenue
							1- Zone d'audit et de traitement des	1- NOV 2017	1- DEC2017	1- DSI	1- A évaluer	1- DSI
							1- Mettre en place un budget pour la définition de la politique informatique					

CESAG - BIBLIOTHEQUE

## **BIBLIOGRAPHIE**

## Ouvrages

1. BERTIN Elizabeth (2007), Audit interne : Enjeux et pratiques à l'international, Editions d'organisation, 320 pages.
2. CORDEL Frédéric et LEBEGUE Daniel, Gestion des risques et contrôle interne : De la conformité à l'analyse décisionnelle, édition Vuibert, 2013, 287 pages.
3. CURABA Sandra, JARLAUD Yannick et CURABA Salvatore (2009), Evaluation des risques, Comment élaborer son document unique ? Paris, Editions AFNOR, 322 pages
4. DARSA Jean-david et Nicolas DUFOUR (2014), le cout du risque : un enjeu pour l'entreprise, Gereso édition, France, 167 pages.
5. DARSA Jean-david (2015,), le facteur risque de l'entreprise : une méthode inédite de mesure des risques de l'entreprise, 2è édition, édition Gereso, France, 219 pages.
6. DE MARESCHAL Gilbert, (2003), La cartographie des risques, Edition AFNOR, Paris, 50 Pages.
7. DEGOS Jean-Guy, le diagnostic financier des sociétés, 2010, édition e-thèque, 119 pages
8. DESROCHES Alain, LEROY Alain et VALLE Frédérique (2003), La gestion des risques, principes et pratiques, Paris, Edition Lavoisier, 286 pages.
9. ERNST & YOUNG (2004), Cartographie des Risques : Convaincre et faire participer sa Direction Générale à cet exercice de management, article : 1-22 pages.
10. FRATTA Hervé, MASSELIN Jean-Luc, MADERS Henri-Pierre, Les métiers d'auditeur interne et de contrôleur permanent, 1<sup>e</sup> édition, édition Eyrolles, 2014, 345 pages.
11. Frédéric BERNARD, Rémi GAYRAUD & Laurent ROUSSEAU (2006), contrôle interne, édition, Edition MAXIMA, Paris 303 pages.
12. GAULTIER-GAILLARD Sophie, Jean-Paul LOUISOT (2014), Diagnostic des risques : identifier, analyser, et cartographier les vulnérabilités, afnor éditions, France, 206 pages.
13. GROUPE PROFESSIONNEL ASSURANCE (2013), Cahier de la recherche : La cartographie des risques, 2ème édition, IFACI, Paris, 136 pages.
14. GROUPE PROFESSIONNEL BANQUE (2013), cahier de la recherche : de la cartographie des risques au plan d'audit, IFACI, Paris, 72 pages.
15. HASSID Olivier (2011), Le management des risques et des crises, 3<sup>e</sup> édition, Dunod, Paris, 180 pages.

16. IFACI (2006), Guide d'audit, Cartographie des risques, Groupe Professionnel Assurance, les cahiers de la recherche, Paris, 70 pages
17. IFACI, PRICE WATER HOUSE COOPERS & LANDWELL& ASSOCIES (2005), Le management des risques de l'entreprise, Cadre de référence, techniques d'application, Editions d'organisation, Paris, 338 pages. (Introduction).
18. JIMENEZ Christian, MERLIER Patrick, DAN Chelly (2008), Risques opérationnels, Edition Revue Banque, Paris, 271 pages.
19. JOKUNG NGUENA Octave (2008), Management des risques, Edition, Paris, 188 pages.
20. KEREBEL Pascal (2007), Mise en œuvre d'un contrôle interne efficace, Edition AFNOR, Paris, 145 pages.
21. KEREBEL Pascal, Management des risques : Inclus secteurs Banque et Assurance, Editions d'Organisation, 2009, 187 pages.
22. KROGERUS Mikael et TSCHAPPELER Roman, le livre des décisions : De Bourdieu au SWOT, 50 modèles à appliquer pour mieux réfléchir, 2012, édition Leduc, 175 pages.
23. LE RAY Jean, De la gestion des risques au management des risques : Pourquoi ? Comment ? édition AFNOR, 2015, 507 pages.
24. LOUISOT Jean-Paul (gestion des risques) 2<sup>e</sup> édition 2014, édition afnor, 265 pages.
25. MADERS Henri Pierre et MASSELIN Jean Luc (2006), Contrôle interne des risques, 2<sup>e</sup> édition, Paris, édition d'organisation, 260 pages.
26. MASSELIN Jean-luc, Maders Henri-Pierre, Contrôle interne des risques : Cibler- Evaluer- Organiser- Piloter- Maîtriser, 2e édition, édition Eyrolles, 2014, 261 pages.
27. MCNAMEE Mac David (1998), Business risk assesment, The Institute of Internal Auditors, Altamonte Spring, 155 pages.
28. MOREAU Franck (2002), Comprendre et gérer les risques, Paris, Editions d'Organisations 222 pages.
29. PIERANDREI Laurent, Risk Management : Gestion des risques en entreprise, banque et assurance, édition Dunod, 2015, 316 pages.
30. PWC- PriceWaterhouseCoopers, IFACI, Coso – Référentiel intégré de contrôle interne : Application au reporting financier externe – Inclus une clé USB avec les outils d'évaluation de l'efficacité d'un contrôle interne, 1<sup>e</sup> édition, édition Eyrolles, 2015, 209 pages.

31. RENARD Jacques (2006), Théorie et pratique de l'audit interne, 6<sup>e</sup> éditions, Editions Eyrolles ,474 pages.
32. RENARD Jacques, L'audit interne : ce qui fait débat, édition Maxima, 2003, 261 pages.
33. RENARD Jacques, Théorie et pratique de l'audit interne : Primé par l'IFACI, 10<sup>e</sup> édition, 2017, édition Eyrolles, 474 pages.
34. SCHICK Pierre, J. VERA, O, BOURROUILH-PAREGE, Audit interne et référentiel de risques, édition Dunod, Paris, 2010, 338 pages.
35. SEAN Cleary, Malleret THIERRY & Schwab K, Risques : perception, évaluation, gestion, 2006, édition Maxima, Paris, 249 pages.
36. TENEAU Gilles et DUFOUR Nicolas (la gestion des risques, un objet frontière) édition l'harmattan, 2013 ,231 pages.

### **Article**

37. NICOLET Marie Agnès et MAIGNAN Michel (2005), Contrôle interne et gestion des risques opérationnels, Revue Banque n° 668, p 51-52

### **Sites internet**

38. COLALTRELLA Thierry (2006), le comité d'audit devra être vigilant sur le contrôle interne, [www.crefige.daufine.fr](http://www.crefige.daufine.fr) [20 janvier 2018]
39. Les Définitions (2011), <http://lesdefinitions.fr/interview#ixzz58gahwZye> [12 février 2018]
40. Les Définitions (2011), <http://lesdefinitions.fr/diagnostic> [28 avril 2018]
41. YAICH A, Le cadre de management des risques de l'entreprise (COSO2) [http://www.larcf.com/seekrcf/RcfPdf/fich\\_085\\_059.pdf](http://www.larcf.com/seekrcf/RcfPdf/fich_085_059.pdf) [12 février 2018]
42. <https://fr.wikipedia.org/wiki/Narration> [12 février 2018]
43. EBONDO WA MANDZILA E & ZEGHAL D, (2009), Management des risques de l'entreprise : Ne prenez pas le risque de ne pas le faire ! <https://www.cairn.info/revue-des-sciences-de-gestion-2009-3-page-5.htm> [10 janvier 2018]
44. KPMG, La cartographie des risques dans le dispositif de gestion des risques, <http://www.audit-commitee-institute.fr>, publié le 01 Janvier 2010

## TABLES DES MATIERES

DEDICACE.....	i
REMERCIEMENTS .....	ii
LISTE DES TABLEAUX.....	iv
LISTES DES FIGURES.....	v
LISTE DES ANNEXES .....	vi
SOMMAIRE .....	vii
INTRODUCTION GENERALE.....	1
PREMIERE PARTIE : CADRE THEORIQUE ET CONCEPTUEL.....	7
CHAPITRE 1 : LE CADRE CONCEPTUEL ET THEORIQUE DE LA CARTOGRAPHIE DES RISQUES.....	9
1.1. Notion du risque .....	9
1.1.1. Définition du risque.....	9
1.1.2. Les types de risques.....	10
1.2. Notion de la cartographie des risques.....	11
1.2.1. Définition de la cartographie des risques .....	11
1.2.2. Les objectifs de la cartographie des risques .....	12
1.2.3. Les acteurs de la cartographie des risques .....	12
1.2.4. Les motivations d'élaboration d'une cartographie.....	13
1.2.5. Les types de cartographie des risques .....	13
1.2.6. Les facteurs clés de succès d'une cartographie des risques .....	13
CHAPITRE 2 : ETAT DE LA LITTERATURE SUR LE DIAGNOSTIC DE LA DEMARCHE D'ELABORATION DE CARTOGRAPHIES DES RISQUES .....	15
2.1. Les différentes approches de cartographie des risques.....	15
2.1.1. L'approche Top down .....	15
2.1.2. L'approche Bottom up .....	15
2.1.3. L'approche combinée.....	16

2.1.4.	L'approche par le benchmarking.....	16
2.1.5.	L'approche par l'autoévaluation .....	16
2.1.6.	L'approche par analyse et synthèse des rationnelles des risques .....	17
2.2.	Les différentes étapes d'élaboration d'une cartographie des risques .....	17
2.3.	Analyse du tableau de synthèse .....	19
2.3.1.	Phase de préparation.....	19
2.3.2.	Phase de planification.....	19
2.3.3.	La phase d'action .....	22
2.3.4.	La phase de reporting .....	23
2.3.5.	La phase de suivi .....	23
2.3.6.	La phase d'actualisation .....	24
2.4.	Diagnostic d'une démarche d'élaboration de cartographies des risques.....	24
2.4.1.	Définition du concept diagnostic.....	24
2.4.2.	Démarche de diagnostic .....	24
<b>CHAPITRE 3 : METHODOLOGIE DE L'ETUDE.....</b>		<b>26</b>
3.1.	Modèle d'analyse.....	26
3.2.	Outils de collecte et d'analyse de données .....	28
3.2.1.	Outils de collectes de données .....	28
3.2.2.	Outils d'analyses de données .....	29
<b>DEUXIEME PARTIE : CADRE PRATIQUE DE L'ETUDE .....</b>		<b>31</b>
<b>CHAPITRE 4 : PRESENTATION DE MARISYS SENEGAL .....</b>		<b>33</b>
4.1.	Présentation du cabinet MARISYS Sénégal .....	33
4.1.1.	Historique du cabinet .....	33
4.1.2.	Missions du cabinet MARISYS .....	33
4.1.3.	Activités du cabinet MARISYS .....	33
4.2.	Organisation du cabinet MARISYS .....	35

CHAPITRE 5 : DESCRIPTION DE LA DEMARCHE D'ELABORATION D'UNE CARTOGRAPHIE DES RISQUES D'UNE DIRECTION DU SYSTEME D'INFORMATION.....	37
5.1. Présentation des différentes phases de l'approche MARISYS.....	37
5.1.1. Phase de planification de la mission .....	37
5.1.2. Phase de formation .....	40
5.1.3. Phase de réalisation .....	41
5.2. Présentation de la matrice.....	69
5.3. Plans d'actions et recommandations.....	71
5.3.1 Plan d'actions.....	71
5.3.2 Recommandations.....	73
CHAPITRE 6 : DIAGNOSTIC DE LA DEMARCHE D'ELABORATION D'UNE CARTOGRAPHIE DES RISQUES.....	76
6.1. Forces et faiblesses de la démarche du cabinet MARISYS.....	76
6.1.1. Les forces de la démarche du cabinet MARISYS.....	76
6.1.2. Faiblesses de la démarche du cabinet MARISYS.....	80
6.2. Recommandations .....	81
CONCLUSION GENERALE.....	84
ANNEXES .....	85
BIBLIOGRAPHIE .....	90