Université Mouloud Mammeri - Tizi-Ouzou

Faculté des Sciences économiques, Commerciales et des Sciences de Gestion

Département des Sciences de Gestion

Filière des Sciences Financières et Comptabilité

Mémoire en vue de l'obtention du diplôme de Master

Spécialité : Audit & Contrôle de Gestion

Intitulé du mémoire :

Audit du processus de gestion des risques opérationnels liés aux systèmes d'informations

Cas de la Banque Nationale d'Algérie (BNA)

Réalisé par :

- BOUDJEMA Thinhinane
- TAZEROUT Lydia

Encadré par :

Mr. MAHTOUT Idir

7ème Promotion

Année universitaire 2020/2021.

REMERCIMENT

Nous tenons à remercier le bon Dieu de nous avoir accordé la santé la force et la volonté d'achever ce travail.

Notre promoteur monsieur Idir MAHTOUT, pour avoir accepté de diriger ce travail, et pour ses conseils, ses recommandations et sa disponibilité tout au long de la réalisation de ce mémoire.

Nos remerciements à l'ensemble au personnel de la BNA, et plus particulièrement à Mme ZEGAI, pour son aide, ses orientations, et pour nous avoir encadré pour réaliser notre cas pratique.

Nos sincères remerciements et notre profonde gratitude s'adressent également à Mme SAHEB, pour ses précieux conseils et ses orientations.

Enfin, nous tenons à remercier tous ceux qui ont contribués de près ou de loin à la réalisation de ce modeste travail et qui se sont dévoués pour nous venir en aide.

Dédicace

Je dédie ce travail à ma maman, mes frères et à ma petite sœur.

À la mémoire de mon père.

À toute ma famille qui m'a toujours encouragé.

À tous mes ami(e)s, spécialement Idir, et ma chère copine Rima.

Et à tous ceux qui m'ont encouragé à braver les difficultés que j'ai rencontré pendant l'élaboration de ce mémoire.

À toutes les lectrices et lecteurs.

Lydia

Dédicace

Je dédie ce travail à mes parents, mon frère, ma sœur et ma tendre tante Malika.

A ma très cher tante Zahra qui a rendu mes études de master possible, et à qui je dois ma réussite.

A la mémoire de ma grand-mère Djedjiga qui rêvait et qui était impatiente de me voir exceller dans mes études.

A mes amies et spécialement Khaled pour m'avoir soutenu, encouragé et tenu la main tout le long de la réalisation de ce mémoire.

Thinhinane

Liste des abréviations

AAA: American Accounting Association

ACPR : Autorité de contrôle prudentiel et de résolution

AICPA: Association of International Certified Professional Accountants

AI: audit interne

AMA: Advanced Measurement Approach

AMF : Autorité des Marchés Financiers

AMRAE : Association pour le Management des Risques et des Assurances de l'Entreprise

AOS: Architecture Oriented Service

ARM: Associate in Risk Management

BA : Banque d'Algérie

BNA : Banque Nationale d'Algérie

BIA: Basic Indicator Approach

BYOD: Bring Your Own Device

CA: Comité audit

CAATs: Computerized Assisted Audit Tools

CBOK: Common Body of Knowledge

CERTS: computer emergency response team security

CI : Contrôle Interne

CIB : Carte Interbancaire

CluSIF : Club de Sécurité des systèmes d'Information Français

CobiT: Control Objectives for Information and related Technology

COSO: Committee of Sponsoring Organization

COCO: Criteria on Control Committee

CMMI : Capability Maturity Model Integration

CSSI : Cellule de Sécurité Système d'Information

DAI : Direction de l'Audit Interne

DCP : Direction de Contrôle Permanent

DG : Direction Générale

DGR : Direction de Gestion des Risques

DRCP : Division Risque et Contrôle Permanent

DSI : Direction des Systèmes d'Informations

DSSI : Direction Centrale de la Sécurité des Systèmes d'Information

EBIOS : Expression des Besoins et Identification des Objectifs de Sécurité

ERM : Entreprise Risk Management

ERP : Entreprise Ressources Planning

FEI : Financial Exécutives International

FERMA : Federation of European Risk Management Associations

GCVP : gestion du cycle de vie d'un produit

IA : Institut des Actuaires

IAE : Intégration d'Application de l'Entreprise

IFA : Institut français des administrateurs

IFACI : Institut Français de l'Audit et du Contrôle Interne

IIA: Institute of Internal Auditors

IMA: Institute of Management Accountants

IRM: Institute of Risk Management

ISO: International Organization for Standardization

IT: Information Technology

IEC: International Electrotechnical Commission

LoD: three lines of defense

MADS : Méthode d'Analyse des Dysfonctionnements dans les Systèmes

MEHARI : Méthode Harmonisée d'Analyse des Risques

MO : Modules Opérationnels

MP : Modules Pilotes

OCTAVE: Operationally Critical Threat, Asset and Vulnerability Evaluation

PGI : Progiciels de Gestion Intégré

PIB : Produit Intérieur Brut

QSE : Qualité-Sécurité-Environnement

RH : Ressources Humaines

RO : Risque Opérationnel

SA : Standardised Approach

SAD : Système d'Aide à la Décision

SEI : Software Engineering Institute

SI : Système d'Information

SID : Système d'Information Dirigeant

SIG : Système d'Information de Gestion

SIS : Système d'Information Stratégique

SMO : Système Management Opérationnel

SO : Système Opérationnel

STT : Système de Traitement des Transactions

TIC : Technologie d'Information et de Communication

TRM: Team Risk Management

TPE: Très Petite Enterprise

USB: Universal Serial Bus

Sommaire

Introduction générale

L’évolution du contexte économique et technologique mondiale ces dernières années, ont accentués le flux d’informations disponibles, et sa valeur n’a fait qu’augmenter au point de devenir une arme contre la concurrence entre les mains de son détenteur. C’est là que le traitement des données, dans le but d'obtenir des informations bien organisées devient essentiel dans de nombreuses organisations et entreprises.

Les progrès des systèmes informatiques ont largement contribué au développement de systèmes permettant la collecte, le stockage, le traitement et l'analyse des données, ainsi que l'extraction et la diffusion des informations à des fins particulières. Ces systèmes sont appelés systèmes d'information « SI » et jouent un rôle important au sein d'une organisation en vue d'accroître l'efficacité de la prise de décision de la direction.

L’immensité des échanges d’informations numériques, notamment grâce à la maturité du marché de l’information et à la multiplicité des technologies de l’information. A fait que les organisations se retrouvent confrontées à une multitude de risques et d'événements inattendus et nuisibles qui peuvent coûter de l'argent ou conduire à une faillite. Ce qui a rendu incertain l’atteinte des objectifs, comme en témoignent les entreprises perturbées par les puissances numériques naissantes, telles que Amazon et Netflix.

Désormais, les organisations sont de plus en plus préoccupées par la protection de leurs systèmes et d'empêcher le vol d'informations. Du coup, elles ont dû améliorer leur jeu afin de mieux protéger leurs informations prioritaires contre les violations de données, les accès non autorisés et d'autres menaces perturbatrices pour la sécurité des données des entreprises et des consommateurs.

C’est là que la gestion des risques prend tout son sens, et joue un rôle essentiel dans la protection des actifs informationnels d'une organisation contre les risques liés à l'informatique, tel que les défaillances matérielles et logicielles, les erreurs humaines, les spams, les virus et les attaques malveillantes, ainsi que les catastrophes naturelles telles que les incendies ou les inondations.

Le concept de « Risk management » en tant que processus qui consiste à identifier, évaluer et contrôler les menaces qui pèsent sur le capital et les bénéfices d'une organisation offre la possibilité d’apporter une réponse efficace aux risques et aux opportunités associées aux incertitudes auxquelles l’organisation fait face, renforçant, ainsi, la stratégie de réduction de la pauvreté et de fournitures de services de qualité des organisations.

Afin de produire un système de gestion des risques efficace, les organisations ont commencé à changer leur approche traditionnelle consistant à gérer les risques séparément d'un département à l'autre, vers un système connu sous le nom de Entreprise Risk Management « ERM » qui intègre tous les processus de gestion de n’importe quel risque, impliqués dans une organisation peu importe sa nature.

Cependant, comme tout système organisationnel, l'ERM peut être défaillant. Les évolutions externes ou internes impactent systématiquement les processus de gestion des risques qui doivent s'adapter en permanence. Afin de s'assurer que ces dispositifs de management des risques remplissent parfaitement leurs rôles, les organisations se dotent d'un outil d'évaluation et de surveillance qui est l'audit interne (Schick et al. 2010).

L'audit interne entre en jeu au début de tout effort de gestion des risques de l'entreprise. Le rôle principal de l'auditeur interne est d'analyser les outils de reporting et les pratiques de gestion des risques existants afin de déterminer s'il existe des lacunes dans les processus de gestion des risques qui pourraient avoir un impact sur les systèmes de contrôle essentiels de l'entreprise.

Problématique :

Dans ce travail, nous tenterons de présenter en détail le rôle et l'avantage qu'offre l'implication des auditeurs interne dans l'ERM pour une organisation, surtout en ce qui concerne la sécurité des SI, en essayant de répondre à la problématique suivante : **Comment l'audit interne contribue-t-il à l'amélioration du processus de management des risques opérationnels liés aux systèmes d'information ?**

De façon plus spécifique nous devons répondre aux questions suivantes :

- Qu'est-ce qu'un SI et quels sont les risques opérationnels que peut engendrer sa mise en place ?

- Quelles sont les méthodes et référentiels promettants la gestion des risques SI ?

- Comment l'audit interne procède-il à l'évaluation de l'efficacité d'un processus ERM ?

Hypothèses :

Afin de mieux cerner notre thématique nous avons émis les hypothèses suivantes :

Hypothèse 1 : l'audit interne fait partie des acteurs de mise en place du processus ERM et suit son fonctionnement en mesurant ses performances.

Hypothèse 2 : l'audit interne améliore le processus ERM en réalisant des missions d'audit de processus pour évaluer sa performance.

Méthodologie du mémoire :

Afin de vérifier la véracité de nos hypothèses et répondre à notre problématique, nous avons diviser notre étude en deux parties.

La première partie qui constituera le cadre théorique de l'étude va nous permettre de cerner les notions de systèmes d'information, de management des risques et d'audit interne et de présenter le rôle principal de l'audit interne dans le management des risques. Ceci à travers une recherche documentaire centré beaucoup plus sur les livres papiers qui traites les thèmes relatifs au management des systèmes d'information, à la gestion des risques opérationnels, à l'audit interne et au rôle qu'il joue dans le management des risques.

Nous avons aussi porter une attention particulière aux thèses, aux rapports, aux documents écris issues de conférences et séminaires, ainsi qu'aux différentes revues académiques qui peuvent apporter des éléments de réponse à notre problématique.

Cette partie comporte deux chapitres de trois sections chacun. Le premier parlera de la notion du système d'information, et des différents risques opérationnels existants dans la section une et deux respectivement. Puis de la gestion des risques opérationnels liés aux systèmes d'informations dans la section trois. Ensuite viendra le chapitre deux qui parlera du processus de management des risques relatif à la norme ISO 31000 « Risk Mangement » dans la section une, puis de la relation entre le processus ERM et le contrôle interne dans la section deux. Pour enfin présenter dans la section trois, le rôle de l'audit interne dans le processus ERM, spécialement dans son évaluation.

La seconde partie qui tient sur un chapitre de trois sections, nous permettra de présenter, s'il existe, le processus de management des risques mis en place par la Banque Nationale d'Algérie, pour parer aux risques de son SI dans la première section, et d'analyser la relation qu'a sa fonction d'audit interne avec ce processus, afin de vérifier la validité des hypothèses émises précédemment dans la dernière section, après avoir présenté la méthodologie de travail dans la seconde section.

CHAPITRE 1 :
Gestion des risques opérationnels des systèmes d'information.

Introduction

L'environnement dans lequel évoluent les entreprises aujourd'hui, complexe et concurrentiel, fait que les informations représentent un véritable actif qu'il faut valoriser et sécurisé. Les systèmes d'information permettent de répondre à ce besoin vital de traitement de flux d'informations de plus en plus croissant qui sont générer au quotidien et ce faisant permettant aux organisations d'assurer leurs développent et leurs pérennités.

Cependant, la mise en place d'un tel système peut entraîner plusieurs défis freinant sa mise en œuvre, et les risques qui émergent ne sont pas des moindres.

C'est pour cela qu'une gestion efficace des risques liés aux SI, et à l'utilisation des technologies de l'information, est plus que jamais essentielle.

Ce premier chapitre va nous aider à prendre connaissance de qu'un système d'information et toutes les notions qu'il lui sont rattachés grâce à la première section. Puis nous allons prendre connaissance de ce qu'un risque, et plus particulièrement qu'est-ce qu'un risque opérationnel et ses typologies.

Enfin dans la dernière section, nous allons prendre connaissances des risques opérationnels liés aux systèmes d'informations, les référentiels et méthodes relatives à leurs traitements, et l'importance d'une bonne gestion des risques au sein des entreprises.

Section 1 : le système d'information organisationnel

Perçu comme une discipline qui s'intéresse aux systèmes d'informations tout en portant une attention particulière aux rôles des informations dans le fonctionnement des organisations, car, qu'elles soient commerciales, comptables ou fiscales, leur traitement est stratégique. Afin de prendre de bonnes décisions, ces informations doivent être de qualité, c'est-à-dire fiables, pertinentes et précises. Dans cette section nous allons aborder la notion du système d'informations, ses types, ses dimensions et son rôle dans l'organisation.

1. L'entreprise système :

Yatchinovsky (2005) défini l'approche systémique comme une approche globale qui fournit une vision globale du système en considérant ses éléments dans leur ensemble et se concentre sur les interactions entre ces derniers plutôt que sur l'analyse détaillée de chacun d'eux.

Le biologiste Bertalanffy (cité par Yatchinovsky, 2005) est le premier à avoir introduit une réflexion sur la notion de système, en démontrant l'importance de l'organisme considéré comme un système dans sa globalité, sa complexité et sa dynamique propre, contrairement à l'approche classique à caractère réducteur.

L'analyse systémique se présente comme une approche alternative et complémentaire à la logique cartésienne, elle rappelle également que tout système repose sur un ensemble de caractéristiques, susceptibles d'établir une typologie des systèmes.

1.1. Les principaux éléments de l'approche systémique selon Yatchinovsky

- **L'interaction** : c'est la relation entre deux éléments sur une double action.
- **La totalité** : c'est-à-dire qu'un système n'est pas la somme de ses éléments, (il est impossible de connaitre les parties sans connaitre le tout, ni connaitre le tout sans connaitre spécialement les parties)
- **L'organisation** : le concept du modèle systémique, c'est un agencement de relation entre les individus, ou un processus par lequel la matière, l'énergie et l'information sont assemblées et mises en œuvre.
- **La complexité** : elle est présente partout et dans tous les systèmes et il est nécessaire de la conserver.

1.2. L'entreprise en tant que système

« Un système est un ensemble de procédés, de pratiques organisées, destiné

à assurer une fonction définie. » (LAROUSSE en ligne, s. d.)

Jean-Louis Le Moigne s'est basé sur cinq points pour dire qu'un système est avant tout un objet appartenant au réel dont on cherche à modéliser, à représenter et à prédire le comportement grâce à des simulations. Cet objet est en interaction avec son environnement et les autres systèmes qui composent ce dernier. Sa finalité est la réalisation d'un profit grâce à une activité créatrice de valeur ajoutée spécifique à ce système et mené par ses acteurs et flux organisés selon sa structure. (M. Gillet, P. Gillet, 2010)

Le domaine de la biologie était le premier à utiliser le concept de système pour expliquer et établir les relations existantes entre les différentes parties d'un corps vivant. Ce qui est nouveau c'est son application au monde de l'entreprise, d'où sa définition comme un ensemble intégré de composantes ou de sous-systèmes visant l'atteinte d'un objectif commun. (Bursh et Felix,
1984)

Globalement, un système est un ensemble complexe d'éléments structurés, organisés, interagissant entre eux afin de réaliser un objectif fixé. Il existait en deux types, un système fermé isolé et dépourvu d'échange d'informations avec son environnement, et à l'opposé on parle maintenant de système ouvert en osmose avec l'environnement.

Apparue au 16ème siècle, l'entreprise est un ensemble d'éléments en interaction dynamique, organisé en fonction d'un but. (De Rosnay, 1975)

D'après l'Institut National De La Statistique Et Des Etudes Economiques, l'entreprise est une unité économique, juridiquement autonome dont la fonction principale est de produire des biens ou des services pour le marché. (Le site de l'INSEE https://www.insee.fr/fr/metadonnees/
définition/c1496)

C'est aussi un regroupement humain hiérarchisé qui met en œuvre des moyens intellectuels, physiques, financiers pour extraire, transformer, transporter et distribuer des richesses ou produire des services, conformément à des objectifs définis par une direction. (Tawfik et Chauvel, 1980)

Conceptuellement, l'entreprise est une institution animée par un plan d'action dans le but de créer des biens et services destinés aux usagers, et ceci en combinat et consommant différentes ressources (matérielles, humaines, financières, immatérielles et informationnelles).

Pour identifier l'entreprise et la distinguer des autres organisations économiques, on doit vérifier si :

- Elle opère sur des marchés et combine les facteurs de production de façon efficiente

et assure la coordination des comportements individuels dans un cadre hiérarchique en tant qu'organisation productive ;

- Elle a une autonomie juridique dans ses décisions ;
- Elle est le cadre de l'activité de l'entrepreneur qui est apte à prendre des risques et à réaliser des innovations.

L'entreprise est une réalité socio-économique qui doit opter pour une des formes juridiques pour exister et se développer au plan légal (Entreprise individuelle, EURL…)
et s'enregistrer auprès des autorités compétentes (Registre du commerce…) pour exister légalement.

L'analyse d'un système voit l'entreprise comme un ensemble de sous-systèmes en interaction qui peuvent être identifiés en fonction du critère retenu : par fonction, par nature de flux, par niveaux, etc…, communiquant entre eux, échangeant des flux de matières, finances ou d'informations.

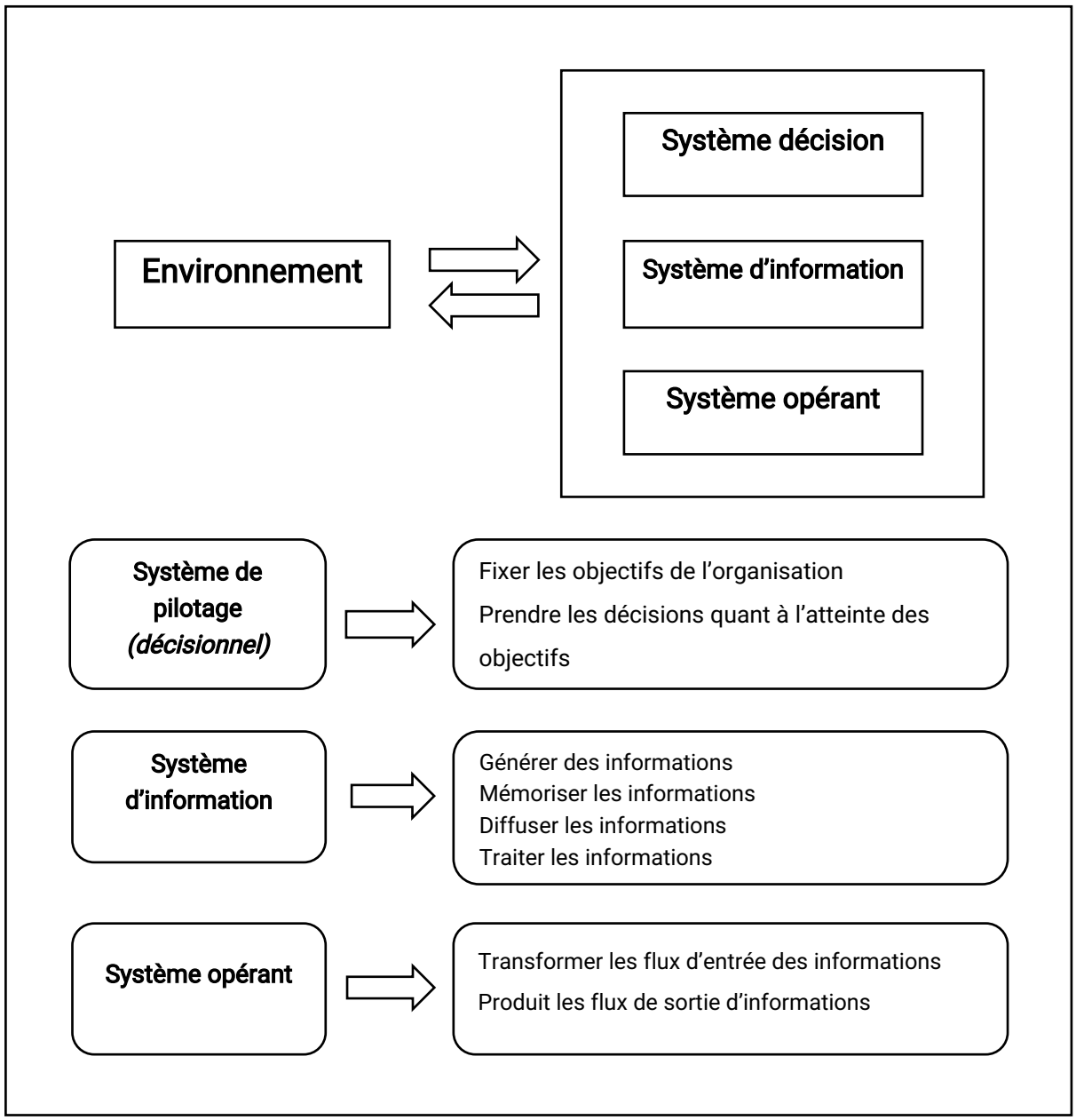
Cet ensemble est organisé pour assurer l'exercice des activités et l'atteinte des objectifs de l'organisation, ce qui rend l'entreprise elle-même un système ouvert, finalisé, régulé.

L'entreprise étant déjà un système, se décompose en 03 sous-systèmes résumés dans le schéma suivant :

Figure (01) : les sous-systèmes, réalisé par nous-même

2. Le système d'information

Souvent associée à la dimension technologique vue l'utilisation d'ordinateurs et de réseaux, la notion du SI est bien plus vaste et recouvre à la fois les dimensions informationnelles, technologiques et organisationnelle.



R. Mason et I. Mitroff (cités par Morley et all, 2011), en prenant en compte le rôle de l'information dans l'organisation, considèrent qu'un système d'information comprend au moins une personne ayant un besoin d'éléments présentés et fournis sous une

forme spécifique au contexte organisationnel dont elle se trouve pour résoudre le ou les problèmes rencontrés. Sous cet angle, le système d'information fait partie du processus de décision sous-jacent et apporte une aide au décideur.

Considérant l'ensemble des activités organisationnelles, G. Davis et M. Olson (cités par Morley et all, 2011), ont défini le SI comme un système qui crée de l'information, grâce à la relation utilisateur-machine intégrée, utile à l'humain pour la prise de décision et l'exécution. Cette définition est aussi limitée à la dimension information.

La définition du SI a pu se développer au fil du temps grâce à R. REIX qui a introduit la notion de procédure dans sa définition, et ceci dans le but de montrer comment, où et quand le personnel va utiliser les ressources du SI pour permettre à l'organisation de rester informée.

A. ALTER a aussi apporté sa touche en intégrant la notion de processus dans la définition d'un SI. Il est parti de la notion de « processus métier » comme un ensemble coordonné d'activités visant à produire un résultat pour des clients internes ou externes, pour dire qu'un SI est une combinaison de pratiques de travail, d'informations, de personnes et de technologies constituant un processus de mise à jour et de diffusion des informations organisées pour atteindre des objectifs dans une organisation. Il appel cette combinaison un « processus travail ». (Morley et all, 2011)

D'une manière générale, un système d'information est un ensemble structuré de ressources matérielles et logiciels (réseaux, serveurs, postes individuels, progiciels, SGBD, applications de gestion, applications métier…), d'acteurs ou utilisateurs, des pratiques de travail (méthodes et procédures internes, ISO 9001, …), de données, de réseaux, dans le but de collecter, traiter, mémoriser, transmettre l'information et la rendre disponible sous différentes formes (données, textes, son, image…) pour l'organisation. (Reix et all, 2016)

Donc, un SI est l'ensemble des flux d'informations circulants à l'intérieur de l'organisation mais aussi avec son environnement externe, associé aux moyens mis en œuvre pour les gérer afin d'atteindre ses objectifs stratégiques correspondants à la stratégie générale de l'entreprise tel que l'utilisation des données clients pour améliorer la politique marketing, ou augmenter la réactivité grâce à un workflow…et son objectif opérationnel qui consiste en l'intégration du SI en tant que support au processus travail, tant au niveau individuel qu'au niveau collectif, selon trois modalités : discrétionnaire (fournir et partager l'information), conseillé (structurer et coordonner le travail), obligatoire (automatiser et intégrer le travail). Et ceci à travers l'accomplissement et l'exécution de ses fonctions qui sont : (Reix et all, 2016)

- Collecter/saisir : acquisition sous la forme adaptée, des données et informations provenant de l'environnement interne ou externe à l'entreprise ;
- Stocker l'information, la rendre disponible et la conserver dans le temps ;

- Transformer/traiter l'information et choisir le support adapté pour la traiter en modifiant le fond ou la forme ;
- Diffuser/communiquer : le SI transmet ensuite l'information dans son environnement interne ou externe.

2.1. Types de systèmes d'information

Un SI dans une organisation peut être décomposer en trois types correspondants aux niveaux organisationnels (stratégie, management et opération). Tout comme on peut approcher les SI selon les fonctions d'une organisation qui sont de quatre (vente et marketing, fabrication et logistique, finance et comptabilité, ressources humaines). Leur but est d'aider les responsables et équipes dans la prise de décision et l'exécution, en fournissant l'information dont l'organisation a besoin pour atteindre son objectif. (K. et J. LAUDON, 2010)

2.1.1. Selon les niveaux organisationnels

- **Le niveau des opérations :**

Caractérisé par les systèmes opérationnel « SO » qui sont un support pour l'exploitation et le fonctionnement des opérations. Leur but est d'aider l'organisation dans le traitement des opérations, des activités et des flux de transactions quotidiennes.

Ces systèmes on les appelle systèmes de traitements des transactions « STT » et leur activité consiste à exécuter et enregistrer les transactions basiques associés aux évènements quotidiens tel que la saisie des bons de commandes. Les STT concernes les opérations internes et externes à l'organisation et produisent une quantité d'informations nécessaires à d'autres systèmes, d'où leur importance et le risque que peux engendrer une panne ou une faille dans ce système.

Domaines fonctionnels	**Ventes et marketing**	**Fabrication et logistique**	**Finances et comptabilité**	**Ressources humaines**	**Autres (spécifique à une industrie)**
Exemples de STT relatives	SI sur les commandes ; Système de support aux ventes…	Systèmes de contrôle machines, achats, qualité…	Grand livre, systèmes de gestion des fonds…	Calcul de la paie, dossiers du personnel…	Exemple d'une université : système d'inscription…

Tableau (01) : exemples de systèmes de traitements des transactions « STT ». Inspiré de « Management des systèmes d'information » de Laudon K. et J. et all. (2010) PP. 53 à 55. Paris : Pearson

- **Le niveau de la gestion :**

Représenté par des systèmes appelés systèmes de managements opérationnel « SMO », Ils transforment des informations opérationnelles en rapports périodiques, pour aider les cadres responsables dans la coordination et le pilotage de l'activité de l'entreprise.

Ces systèmes sont divisés en deux groupes : les SI de gestion « SIG » et les systèmes d'aide à la décision « SAD ». Les SIG utilisent les données internes des STT et les transformes en rapports périodiques afin d'aider les cadres intermédiaires à répondre aux questions routinières, en suivant des procédures prédéfinis Puis les SAD regroupes, en plus d'informations externes, les données des STT et les résultats des SIG pour formuler des rapports spéciaux utiles aux cadres intermédiaires et aux experts.

Caractérisés par leurs grandes puissances analytiques dans le traitement de grandes quantités de données maniables, les SAD permettent aux gestionnaires de connaître les détails importants d'une situation pour optimiser la planification, la prise de décisions, l'atteinte des objectifs et la supervision des opérants.

La comparaison entre les résultats des SAD et des SID aident les cadres supérieurs à optimiser le processus décisionnel pour un meilleur résultat.

- **Le niveau stratégique** :

Représenté par des systèmes d'informations stratégiques « SIS » qui facilitent la prise de décision par la direction. Ils sont matérialisés par des systèmes qui aident les dirigeants dans le pilotage global de l'organisation, appelés SI pour dirigeants « SID ».

Ils regroupent, en plus des données externes, les informations traitées et résumées par les SIG et SAD. Ces données sont filtrées et transformées en graphes par les SID, accessibles par une interface web, utilisés pour réduire les incertitudes décisionnelles concernant l'avenir de l'entreprise et l'amélioration des perspectives et performances de l'entreprise.

2.1.2. Selon un point de vue fonctionnel

- **Systèmes de vente et de marketing** : ils regroupent les données de chaque

niveau de l'organisation pour un pilotage optimale des activités commerciales (clients potentiels, études de marché, concurrences…)

- **Système de fabrication et de logistique** : exemple du « GCVP » SI de gestion de cycle de vie d'un produit, il permet surtout aux entreprises industrielles, de réduire les coûts liés au prototypage, et aussi de gérer les approvisionnements, exécuter les commandes et gérer les changements relatifs.

- **Systèmes des activités financières comptables** : pour établir les prévisions à long terme, gestion des ressources financières et le suivit des mouvements des fonds de l'entreprise.
- **Systèmes des ressources humaines** : concernent la tenue de dossiers complets et la création de programmes pour la main-d'œuvre (recrutement, perfectionnement et maintien)

2.2. L'intégration d'un SI dans une organisation

L'intégration dans les SI fait référence au fait de regrouper les données de tous les systèmes, les transformer, et présenter les informations nécessaires rapidement grâce à la cohérence, la communication et la synchronisation en éliminant les activités inutiles (recherche, saisie, transmission…), aux acteurs sous la forme voulue.

Un SI intégré dans une entreprise est un système capable de regrouper les informations de l'ensemble des domaines fonctionnelles et unités organisationnelles dans le but de coordonner l'ensemble des processus et actions de cette entreprise avec ses partenaires (fournisseurs, clients…). La nécessité d'intégrer les SI vient de la disparaissions des systèmes isolés, et de la volonté d'obtenir des informations fiables et rapidement, et ceci pour augmenter la réactivité (juste à temps).

Une intégration efficace nécessite une communication codifié propre à l'organisme, de l'information véhiculé qui est censé être pertinente, structuré et cohérente. (Tassin, 2005).

2.2.1. Les pratiques d'intégration

Pour Thevenot (2011), l'intégration d'un SI doit être perçu tel un mode d'organisation logique, car elle passe par l'utilisation des outils et technologies supports comme les progiciels de gestion intégrés ou les « Entreprise Resource Planning » (PGI / ERP) qui sont de type modulaire et qui reposent sur une base de

données unique car elle est le pivot du système et le vecteur de l'intégration.

Les PGI ont trois types de modules déployables à savoir les génériques tel que ceux utilisé dans la comptabilité, contrôle de gestion, ressources humaines…, les modules utilisés à l'industrie comme la planification ou l'ordonnancement, et enfin les modules destinés aux services.

Il existe aussi des intégrations d'applications de l'entreprise (IAE) qui sont un outil d'intégration essentiel se résumant à une couche de logiciels « middleware » se plaçant au milieu des applications à interconnecter, cet outil a l'avantage de préserver l'existant au sein du SI.

Les entrepôts de données ou le (Data Warehouse) sont essentiellement un projet de mise en cohérence des données et l'intégration, ils reposent sur la structuration de ces dernières et sur leur historisation et la traçabilité des opérations les concernant au sein des diverses bases de données.

Une architecture orientée services (AOS) est destinée à améliorer la flexibilité opérationnelle du système d'informations, elle permet aussi d'optimiser l'utilisation des ressources existantes et de minimiser les couts de développement et de déploiement des éventuelles nouvelles applications en modélisant et mutualisant les processus métiers majeurs pour mieux les pérenniser. L'idée est de faciliter les opérations d'adaptation inéluctables lorsque le métier de l'entreprise et les données contextuelles de l'environnement évoluent. (Thevenot, 2011)

2.3. Dimensions d'un SI

Pour mieux comprendre la notion de système d'information, il est primordial de le considérer comme un système multidimensionnel qui se compose de trois différentes dimensions : (Reix et all, 2016)

2.3.1. Une dimension informationnelle/management :

Chaque responsable a besoin d'un certain nombre d'informations spécifiques à sa position hiérarchique dans l'organisation qu'il peut se procurer que par le billet d'un SI.

Le premier objectif d'un SI est de représenter l'information de manière accessible. Cette représentation doit être pertinente et de qualité car elle influence le comportement (décisions) des utilisateurs.

Ce qui explique l'importance de la communication et le partage des connaissances, des modèles, des concepts et langages utilisés dans la représentation qui est définit par J. C. Abric comme un système de prédécodage de la réalité qui détermine les

anticipations et les ententes. C'est donc une image du monde réel, d'un ou d'un évènement afin d'atteindre un but bien précis qui est d'assurer la conservation, la communication et la concrétisation de l'information par des modèles.

L'utilisation des représentations peut avoir des conséquences et des risques de distorsion car elles peuvent être créées par les utilisateurs ou bien des tiers, comme par exemple le comptable qui rédige le bilan à la fin d'un exercice pour un client.

Une représentation est pertinente quand elle répond aux besoins de son utilisateur dans un contexte particulier. Cette pertinence est déterminée par 8 points résumés par la figure suivante. Elle dépend aussi de la valeur et du coût d'obtention de l'information utilisé pour la représentation.

2.3.2. Une dimension technologique

Les SI étant une construction désormais fondée sur une architecture technologique, ils utilisent différentes technologies numériques pour saisir, stocker, traiter et communiquer l'information sous forme de données symbolisées.

Cette technologie se compose de matériels informatiques et de télécommunications ; postes de travail (clavier, écrans, USB…), serveurs et logiciels.

L'informatisation des SI a permis de compresser le temps de traitement des données et l'espace qu'elles occupent. Faciliter l'utilisation, la modification et le transport d'énormes quantités de données, et aussi assurer la connectivité et la mobilité (Transfer et accès aux données sur différents endroits connectés entre eux).

2.3.3. Une dimension organisationnelle

Pour un SI fonctionnant dans une organisation, sa dimension organisationnelle peut être analyser selon deux perspectives relatives au fonctionnement et la structure de l'organisation, sachant que le système d'information est un élément constitutif de l'organisation.

Par rapport à la perspective de fonctionnement, celle-ci regroupe le déroulement des activités, des événements et des résultats de chaque processus, ainsi que la coordination entre ces processus. Mais aussi la gestion commerciale et marketing de ses fonctions grâce à l'information des gestionnaires et à la gestion et la communication de la connaissance.

2.4. Rôles et moyens d'un SI.

Pour M. et P. GILLET (2010), le rôle d'un SI se résume en trois points :

- Le SI est un instrument de couplage entre les modules opérationnels et les modules pilotes au sein de l'organisation, car il permet une prise de décision efficace et une réaction rapide aux changements de l'environnement. Les

résultats dépendent de la qualité de ce couplage en ce qui concerne la fiabilité et la rapidité de transmission de l'information, sa complétude et son accord par rapport aux besoins du destinataire ;

- Le SI, considéré comme étant la mémoire de l'organisation, est un outil de communication entre les différents services d'une entreprise grâce à des flux d'informations en interne permettant d'analyser son propre fonctionnement, mais aussi en externe (fournisseur, client, autres SI…).

  Il a donc un rôle opérationnel et stratégique dont la finalité est de préserver la mémoire de l'organisation qui constitue son histoire, son savoir et son savoir-faire. Pour ce faire, l'organisation doit investir dans un bon SI capable non seulement de stocker l'information qui constitue sa matière première, mais aussi de la mettre à disposition en cas de besoin. Donc, le système d'information est la mémoire, les oreilles, et la parole de l'organisation ;

- Le SI met en forme des données d'une façon adaptées aux besoins de l'entreprise, et les fait circuler conforment aux besoins du destinataire et adapté à sa position et son rôle dans l'organisation. Cela permettra à chaque acteur de répondre aux types de questions qu'il rencontre dans l'exercice de son poste de travail au bon moment.

En résumé, le système d'information permet au système opérant de communiquer des informations qui ont été collectées et modifiées au système de pilotage qui est en charge de contrôler et prendre des décisions afin d'améliorer la productivité.

2.4.1. Les moyens d'un SI

M. et P. GILLET (2010) ont proposé les moyens ci-dessous :

- **Les ressources humaines** : l'acteur humain constitue la ressource première de tout systèmes d'information car il est au centre de la création de l'information. Tout individu salarié d'une organisation fait forcément partie de son SI.

- **Les ressources matérielles** : il s'agirais donc de toute l'infrastructure technologique tel que les ordinateurs, les moyens d'impression, les câblages, les serveurs, les stations de travail…etc. Bien plus que ça, l'agencement des bureaux ou même les panneaux d'affichage sont des éléments constitutifs du SI. Il est

donc à constater que tout moyen physique aidant et faisant part au SI est considéré comme ressources matérielle.

- **Les ressources immatérielles** : ou bien simplement l'aspect logiciel du SI, donc il s'agit de l'ensemble de l'architecture applicative d'une organisation.

- **Les ressources financières** : malgré l'aspect immatériel de l'information, son management s'avère fort couteux. Quand le service financier tente de calculer le retour sur investissement des technologies de l'information, cela représente très souvent un problème.

L'écart entre l'amélioration de la productivité des ordinateurs et celle des salariés est nommé « paradoxe de SOLOW », est mis en avance par le professeur américain Robert SOLOW et durant ces années passées il n'a fait que s'amplifier en raison du décalage dans le temps entre l'investissement en connaissances et son impact, dû au temps de formation et aux effets d'obsolescence. Les technologies visant la gestion des informations sont un moyen nécessaire aux organisations, et ce peu importe leur coût.

2.5. Caractéristiques d'un SI.

Afin qu'il ait des possibilités de satisfaire les besoins de l'organisation, il existe plusieurs interactions mises en œuvre au sein du système d'informations, et ce en véhiculant différentes informations principalement entre les modules opérationnels et les modules pilotes. M. et P. GILLET (2010) montrent ces différentes interactions sous formes d'axes dans la figure ci-dessous :

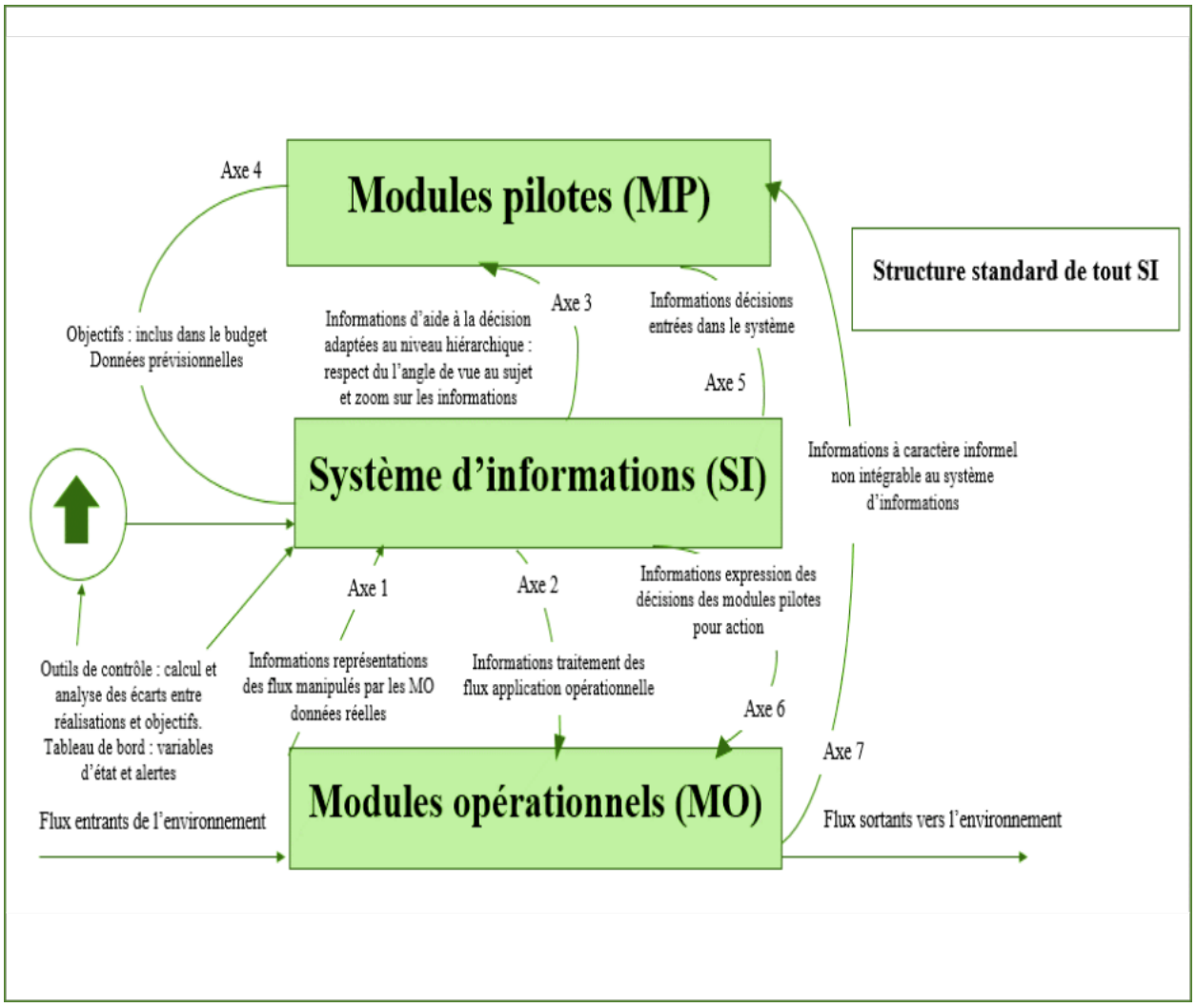


Figure (02) : Les flux d'information d'un SI à partir de « Système d'information des ressources humaines », M. et P. GILLET, 2010, p. 28, Dunod

- **1er Axe des informations sur les représentations des flux du module opérationnel :**

Les modules opérationnels (MO) doivent collecter des informations et les intégrer dans le SI, afin que ces dernières accompagnent l'action réalisée sur les flux matériels, monétaire ou humains lors de leurs transformations en flux sortants. Les modules opérationnels auront donc pour tâche de permettre au système

d'information l'acquisition immédiate et complète de ces flux de données.

- **2eme Axe des informations sur le traitement des flux :**

Le système d'informations va permettre de traiter les flux d'informations volumineux et répétitifs, qui sont liés à la transformation des flux entrants en flux sortants par les modules opérationnels. Ces données sont la source de l'information des modules pilotes. Elles leur permettront de comparer les objectifs assignés avec les réalisations et de prendre des décisions pour les orientations à venir de l'organisation.

- **3eme Axe des informations d'aide à la décision :**

Le système d'informations, en plus de faire circuler les informations lors du couplage entre les deux modules opérationnel et pilote, il fait en sorte également de rendre les informations plus ou moins synthétiques et les adapter au point de vue du destinataire. Car, au même niveau hiérarchique, les différents acteurs ont besoin d'informations différentes puisqu'ils n'ont pas les mêmes rôles. Le SI va également permettre de diffuser auprès des décideurs des informations pertinentes, avec un délai suffisamment bref et sans déformation.

- **4eme Axe des informations concernant les objectifs assignés :**

Le système d'informations doit intégrer des données prévisionnelles qui constituent des objectifs, ensuite il les mémorisera et contrôlera. Ces objectifs sont fixés par le module pilote, et ce grâce à la démarche budgétaire. Cette dernière a pour mission la définition des objectifs à atteindre et leurs répartitions au niveau de responsabilité de chacun.

- **5eme Axe des informations concernant les décisions prises par les MP :**

En s'appuyant sur les informations fournies, les modules pilotes vont pouvoir prendre des décisions, mais cela ne suffit pas car ce qui est plus difficile c'est l'obtention de leurs transformations en actions. C'est la raison pour laquelle il faut que les acteurs opérationnels chargés de ces transformations, soient informés de la décision. Il est donc nécessaire d'intégrer les décisions dans le SI.

- **6eme Axe des informations d'expression des décisions prises par les MP :**

Le SI permet la transformation des décisions globales en informations opérationnelles adéquates pour l'action. Ces décisions doivent être détaillées et traduites par rapport aux conséquences qu'elles peuvent entraîner pour chaque module opérationnel. Ensuite, afin d'assurer le couplage entre MP et MO, le SI doit être correctement structuré.

- **7eme Axe des informations informelles non intégrables dans le SI :**

Les données acquises en dehors de l'intervention du SI par les modules

opérationnels circulent de manière informelle, c'est-à-dire sans aucune adaptation, ni délai, ni fiabilité et parfois avec des distorsions. Il en est de même pour les décisions prises par les modules pilotes, qui doivent être transmises aux modules opérationnels pour action.

Cependant, certaines informations ont, par nature, un caractère informel et s'appuient sur des relations interpersonnelles qui rendent impossible, et même non souhaitable, l'intervention du système d'information dans leur circulation. Elles doivent conserver leur caractère de subjectivité.

2.6. Qualités et limites d'un SI

Elles sont introduites par M. et P. GILLET (2010) comme suit :

- **La rapidité et la facilité** :

Ce critère est considéré par rapport au temps maximum tolérable de la circulation d'une information pour que les décisions et les actions qu'elles entraînent, soient effectuées dans des délais compatibles. Il s'agit donc de posséder la bonne vitesse de transmission de l'information pour chaque donnée en fonction du moment considéré et en fonction de la nature de l'information elle-même.

- **La fiabilité** :

C'est une qualité qui doit être absolue. Afin qu'une information soit sure et fiable, elle doit d'abord être pertinente et complète, lors de son acquisition, et qu'elle doit ensuite être transmise sans déformation et sans déperdition, tout au long du circuit.

  - La pertinence de l'information est le premier critère de fiabilité et il exige la présence de l'information dans le système, que dans la mesure où elle le concerne (l'information est filtrée en fonction de l'utilisateur).

  - Le critère de complétion de l'information exclue toutes informations partielles qui ne peuvent pas être traitées ou qui peuvent entraîner des erreurs de traitement.

- **L'intégrité** :

Le SI permet l'intégrité des informations en les maintenant dans un état cohérent tout en s'assurant de pouvoir réagir à des situations qui peuvent rendre les informations incohérentes.

- **La sécurité** :

Le SI s'assure de la protection des informations et ce en les sauvegardant en premier lieu et en prévoyant la malveillance et les attaques extérieurs grâce à des routeurs filtrants, des anti-virus, des pares-feux, des détecteurs d'intrusions… etc.

- **La confidentialité** :

C'est un aspect crucial que le SI procure à l'information pour faire face à l'espionnage industriel et ce en mettant en place les meilleurs moyens matériels et immatériels.

2.6.1. Ses limites

Il existe dans l'organisation des informations subjectives et appartenant au domaine des relations humaines qui ne concernent pas le système d'information. Elles peuvent être parfois très importantes et contribuent à expliquer le fonctionnement de tel service ou de telle entreprise, mais le système d'information ne peut en rendre compte. (M. et P. GILLET, 2010)

Certaines informations ne peuvent pas être traitées de manière automatisée ou informatisée, car elles ne sont pas reproductibles et codifiables et elles ne présentent pas de caractère de répétitivité. Ces informations peuvent avoir une incidence sur le long terme et sur la stratégie, elles doivent cependant être prises en compte par les modules pilotes dans leur processus de décision.

Grace aux outils informatiques, certaines informations dans le SI peuvent faire l'objet d'un traitement automatisé. Il s'agit des informations volumineuses et répétitives, comme le traitement des commandes clients et fournisseurs par exemple.

La procédure de traitement de chacune des informations est définie à l'avance de manière formelle et explicite, sous forme de règles de gestion standards à appliquer, en fonction des différentes situations possibles, qui seront toutes envisagées.

Il est important de savoir distinguer entre un domaine automatisable et un domaine automatisé, car cela permet de différencier les données informatisées de celles qui subissent en traitement manuel. (M. et P. GILLET, 2010)

3. L'infrastructure technologique d'un SI

L'une des composantes maîtresses de la performance opérationnelle d'une

entreprise, elle concerne tout investissement en matériels, logiciels et services associés, dirigé par les managers et incluant les RH et techniques permettant l'optimisation du fonctionnement de l'organisation. (K. et J. Laudon et all, 2013)

3.1. Informatique, processus métier et SI

Le SI ne doit pas être confondu avec le système informatique car il en est un sous-ensemble du système d'information qui regroupe l'ensemble des moyens informatiques nécessaires au traitement de l'information. Il n'est que le support du système d'information.

L'informatique pour LAROUSSE en ligne (s.d.) c'est la science du traitement automatique et rationnel de l'information en tant que support des connaissances et des communications qui met en œuvre des matériels et des logiciels.

Aujourd'hui on parle de système informatique car il ne s'agit plus de couvoir l'aspect technique des technologies et des applications de l'information, mais de couvrir en même temps son aspect infrastructure matérielle et logiciel. Comme le précise la définition de Morley et all (2011, p. 28) « Un système informatique est un ensemble organisé d'objets techniques, matériels, logiciels, applicatifs qui représente l'infrastructure d'un système d'information »

3.1.1. La distinction entre SI et informatique

INFORMATIQUE	SYSTEME D'INFORMATION
Un outil, un moyen Un centre de coûts	Un élément de création de valeur, un actif.
Fonction automatiser Fonction transversale de support.	Fonction de transformation stratégique.
Approche fonctionnelle qui consiste à identifier des besoins opérationnels et informationnels immédiats et leur fournir des fonctionnalités et des solutions à court terme	Approche informationnelle dont le but est de comprendre le métier de l'entreprise afin de construire ou de reconstruire des fondations durables pour son système d'information.

Dans un projet, le maître d'œuvre est responsable de la conception et la construction du système informatique	Il est du domaine de l'entreprise globale, et dans un projet, le maître d'ouvrage et le maître d'œuvre sont tous deux responsables de la définition et la mise en œuvre du système d'information.

Tableau (02) : Distinctions entre informatique et système d'information à partir de « Le système d'information nouvel outil de stratégie », Deyrieux A., 2004, p12, Maxima.

3.1.2. Processus métier et SI

L'ISO 9000 ; 2000 définis un processus comme étant un ensemble d'activités corrélées ou interactives qui transforme des éléments d'entrée en éléments de sortie. Morley et all (2011) propose une définition plus orienté métier et SI qui se caractérise par son unification qui permet flexibilité aux interprétations et décisions des acteurs.

Un processus est un ensemble d'activités, entreprises dans un objectif déterminé. La responsabilité d'exécution de tout ou partie des activités par un acteur correspond à un rôle. Le déroulement du processus utilise des ressources et peut être conditionné par des événements, d'origine interne ou externe. L'agencement des activités correspond à la structure du processus. (P. 49)

Pour Morley et all, un processus métier est un groupe d'opérations et d'activités mises en relation logique entre elles pour avoir un résultat voulu, il organise le travail des acteurs pour répondre à des objectifs définis par la stratégie. Il est composé par un ou plusieurs processus système d'information qui s'occupent de structurer l'utilisation et la mise en disposition de l'information, selon le processus métier auquel il correspond.

Les processus SI sont mis en œuvre par des processus informatiques représentés par un ensemble d'activités logicielles, exécutées par des machines, utilisant des objets informatiques, pour atteindre un objectif de traitement informatique précis. (Morley et all)

La modélisation des processus métiers et des processus systèmes d'information est communes, sauf que les processus informatiques requièrent une plus grande formalisation, notamment pour décrire les objets utilisés, les événements et conditions, ainsi que les traitements élémentaires. (Morley et all)

- **Les processus principaux :**

Générateurs de valeur et d'avantage stratégique, ils sont au cœur de l'organisation. Leur résultat s'adresse à un client ou un partenaire externe et ne sont pas transposables d'une Organisation à l'autre. Ils donnent lieu à une modélisation détaillée.

- **Les processus secondaires :**

Nécessaires à l'exécution des processus principaux (états comptables, paye...). Ils sont sources de coût sans création directe de valeur, et peuvent s'adapter dans le cas d'intégration d'un progiciel.

- **Les processus de pilotage :**

Ont pour but de contrôler l'atteinte des objectifs et la mise en œuvre de la stratégie de l'entreprise. Ils sont traduits par des tableaux de bord (suivi des ventes, suivi du taux de remplissage, suivi des réclamations...). Par exemple, le processus qualité et un cas particulier de processus de pilotage. Son but est de vérifier qu'un processus a été correctement défini.

3.2. Composantes de l'infrastructure technologique d'un SI

K. et J. LAUDON (2010) ont parlés de 7 composantes reliés entre elles et que les entreprises doivent y investir pour en tirer la meilleure des compositions dans la cohérence et la fiabilité à longue durée. Nous synthétisons ces composantes dans le tableau ci-dessous :

Composantes technologiques d'un SI	Etude des marchés concernés	Principaux fournisseurs
Plateformes matérielles	Comprend des ordinateurs clients et des serveurs qui ont pu se développer et être compatible avec l'activité des grandes entreprises grâce à l'apparition des data center.	**Machines :** HP, IBM, Dell, Sun Microsystème… **Processus:** Intel, IBM, Samsung, Toshiba…
Plateformes du système d'exploitation	WINDOWS de Microsoft domine le marché des ordinateurs clients en tant que système d'exploitation, alors que les entreprises optent pour des systèmes économiques tel que UNIX ou le logiciel libre LINUX ou OpenOffice d'Oracle (2009).	Pour UNIX on a IBM, HP, Dell, Sun

ERP	Utilisés par les grandes entreprises vue la difficulté et leur leurs coûts d'intégration. Le reste optent pour des EAI (intégration d'applications d'entreprises) en tant que *midleware* pour éviter les risques liés aux changements ou modernisations de leurs systèmes informatiques.	**Moyennes et grandes entreprises :** SAP, Oracle **Entreprises modestes :** Microsoft, Generix et Sage
Organisation et stockage des données	Il s'agit de logiciels responsables de l'organisation et de facilitation d'accès et d'utilisation technique et efficace des données.	**Logiciels :** IBM, Oracle, Microsoft, Sybase. **Matériels :** EMC Corporation, IBM, HP puis Western Digital, Seagate, Hitachi, Toshiba/Fujitsu et Samsung pour les disques dures.
Equipements réseaux et télécommunications	Un marché en expansion grâce aux technologies WI-FI et téléphonies mobiles et sur internet.	**Matériel :** Cisco, Juniper, Alcatel -Lucent ; Services et **télécommunications :** MCI, AT&T…
Plateformes internet	Permet de réduire le nombre de serveurs utilisés tout en augmentant leur taille et puissance grâce aux services d'hébergements web.	Microsoft FrontPage, Microsoft.NET, Sun (Java) et d'autres développeurs de logiciels tel que Macromedia (Flash)…
Services de conseil et intégrations des systèmes	Un marché lucratif vue les risques et le gouffre financier qu'un changement de système ou l'intégration d'un nouveau peut engendrer.	Ce sont les fournisseurs de matériels et logiciels qui concluent des alliances avec des professionnels dans le domaine comme IBM, Oracle et SAP.

Tableau (03) : Composantes de l'infrastructure technologique d'un si. Inspiré de « Management des systèmes d'information » de Laudon K. et J. et all. (2013). PP. 174 à 178. Paris : Pearson

Section 2 : le risque opérationnel d'une entreprise

La question du risque devient un enjeu essentiel aujourd'hui dans l'entreprise car il n'y a ni croissance ni création de valeur sans sa prise. Il existe divers

risques auxquels l'entreprise fait face, et qui peuvent remettre en cause sa pérennité au quotidien. Le risque opérationnel résultant du « cœur opérationnel » de l'entreprise est l'un des risques les plus complexes car il est extrêmement large. Dans cette section nous allons nous approfondir sur les notions fondamentales du risque opérationnel.

1. La notion du risque.

L'IIA parle du risque comme la possibilité que se produise un événement susceptible d'avoir un impact sur la réalisation des objectifs. Pour l'IFACI, le risque est un ensemble d'aléas susceptibles d'avoir des conséquences négatives sur une entité et dont le contrôle interne et l'audit ont notamment pour mission d'assurer autant que faire se peut la maîtrise. Bien qu'il soit défini souvent comme cette possibilité, son existence est liée seulement à l'atteinte d'un objectif donné. (Schick et al, 2010)

D'après Larousse en ligne (s. d.), il s'agit d'un danger, d'un inconvénient plus ou moins probable auquel on est exposé, et il précise qu'il constitue un préjudice, un sinistre éventuel que les compagnies d'assurances garantissent moyennant le paiement d'une prime.

Toutes ces définitions mettent en évidence les composantes du risque à savoir la gravité ou conséquences de l'impact et la probabilité qu'un ou plusieurs événements se produisent.
Ces composantes sont clairement mises en évidence par la définition ISO du risque comme
étant **«** la possibilité d'occurrence d'un événement ayant un impact sur les objectifs. Il se mesure en termes de conséquences et de probabilités ». (Schick et al, 2010)

Schick a précisé qu'il n'y a de risque que par rapport à l'atteinte d'un objectif ou plus précisément que par rapport à la conséquence dommageable de ce risque quant à l'atteinte d'un objectif. « Le risque est un concept signifiant la possibilité que la combinaison d'un événement incertain et d'un mode de fonctionnement aléatoire ait pour conséquence le non atteint d'un objectif *».* (2010, p.11)

Ce schéma résume la conceptualisation et la définition du risque :

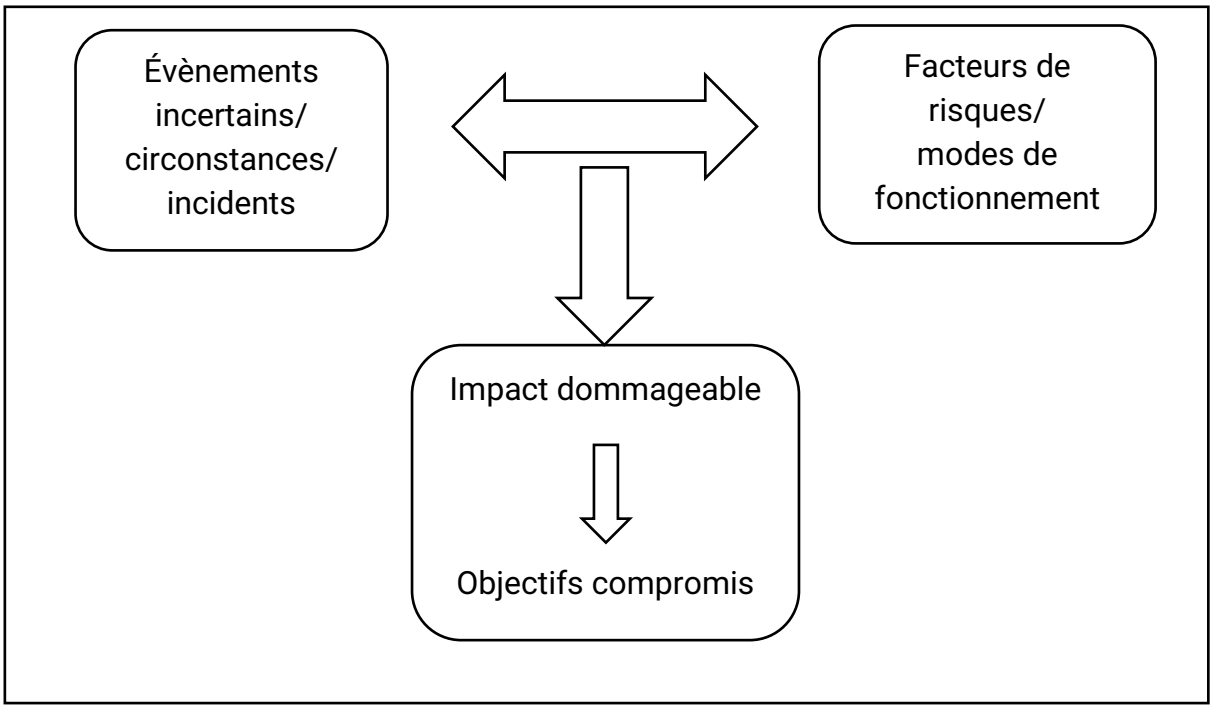


Figure (03) *:* Conceptualisation et définition du risque. A partir de « Audit interne et référentiels de risque » de Schick et all (2010). P. 11. Paris : Dunod

1.1. Distinction entre le risque, le danger et la menace.

Il existe des similitudes entre ces trois termes n'exprimant pas les mêmes idées, qui génèrent souvent des confusions, notamment entre le risque et la menace.

La menace et le danger eux, ils expliquent la séquence de causalité du risque, car la menace amène le danger, qui, une fois concrétisé, engendre potentiellement un risque.

Précédemment nous avons défini le risque comme la probabilité ou l'éventualité de la réalisation d'un événement plus ou moins prévisible mais qui est indésirable dans le sens « hasard » ce qui le différencie de la menace qui peut être associée au terme « avertissement » car il s'agit d'un indice ou d'un signe qui laisse prévoir un danger.

Quant au danger, il est défini comme la remise en cause de l'intégrité de quelque chose, selon le modèle d'évaluation des risques MADS « Méthode d'Analyse des Dysfonctionnements dans les Systèmes » le danger est « tout phénomène, situation ou événement potentiel ; déclenché par une ou plusieurs événements déclencheurs, susceptible de menacer une ou plusieurs cibles ». (Schick et all, 2010)

1.2. Le risque entre danger et opportunité.

Le risque est lié à la prise de décision qui a pour objet à soumettre une cible à un danger. Le danger est une propriété intrinsèque à une source de danger. (MAZOUNI,

2008) donne une définition intéressante aux concepts de risque et de danger :

Le risque constitue une potentialité. Il ne se réalise qu'à travers la réunion et la réalisation d'un certain nombre de conditions et la conjonction d'un certain nombre de circonstances qui conduisent, d'abord, à l'apparition d'un ou plusieurs éléments initiateurs qui permettent, ensuite, le développement et la propagation de phénomènes permettant au danger de s'exprimer, en donnant lieu d'abord à l'apparition d'effets et ensuite en portant atteinte à un ou plusieurs éléments vulnérables. (Pp.28, 29)

Néanmoins, le risque ne se rattache pas forcément à l'occurrence d'un événement malheureux, ou à un danger, il peut être une opportunité pour apprendre à mieux connaître les lacunes de la stratégie suivie par une société qui évolue vers ses objectifs tout en préservant son image de marque, sa qualité de service, et intrinsèquement l'ensemble des enjeux sociaux, économiques, techniques, financiers, juridiques, etc. Justement, le retour d'expérience est une perception intelligente de la notion de risque qui consiste d'ailleurs à tirer profit de l'occurrence de certains événements indésirables. (MAZOUNI, 2008)

1.3. Typologies du risque.

Il existe plusieurs centaines de risques susceptibles de fragiliser, voire de remettre en cause la pérennité des entreprises. Treize principales classes de risques sont en présence au sein des organisations qu'on analyse particulièrement due à leurs enjeux, à savoir les risques géopolitiques en premier lieu, les risques économiques, les risques stratégiques et les risques financiers. Puis nous avons les risques industriels et les risques opérationnels, ces derniers comprennent trois catégories qu'on traite d'une manière différenciée à savoir les risques juridiques, les risques informatiques et les risques ressources humaines. (Darsa, 2013a)

Les risques d'image et de réputation aussi prennent place dans cette liste aux cotés des risques de gestion de la connaissance. Enfin nous avons d'autres risques de multiples sources et les risques d'intégrité qui viennent en dernier.

Darsa les a placés sur une pyramide des risques suivant un ordre rationnel, le risque concerne un individu au sommet de la pyramide et le groupe à la base lors d'une lecture de haut en bas, à l'inverse pour une lecture de bas en haut, le risque est au niveau macroéconomique à la base et au niveau microéconomique au sommet.

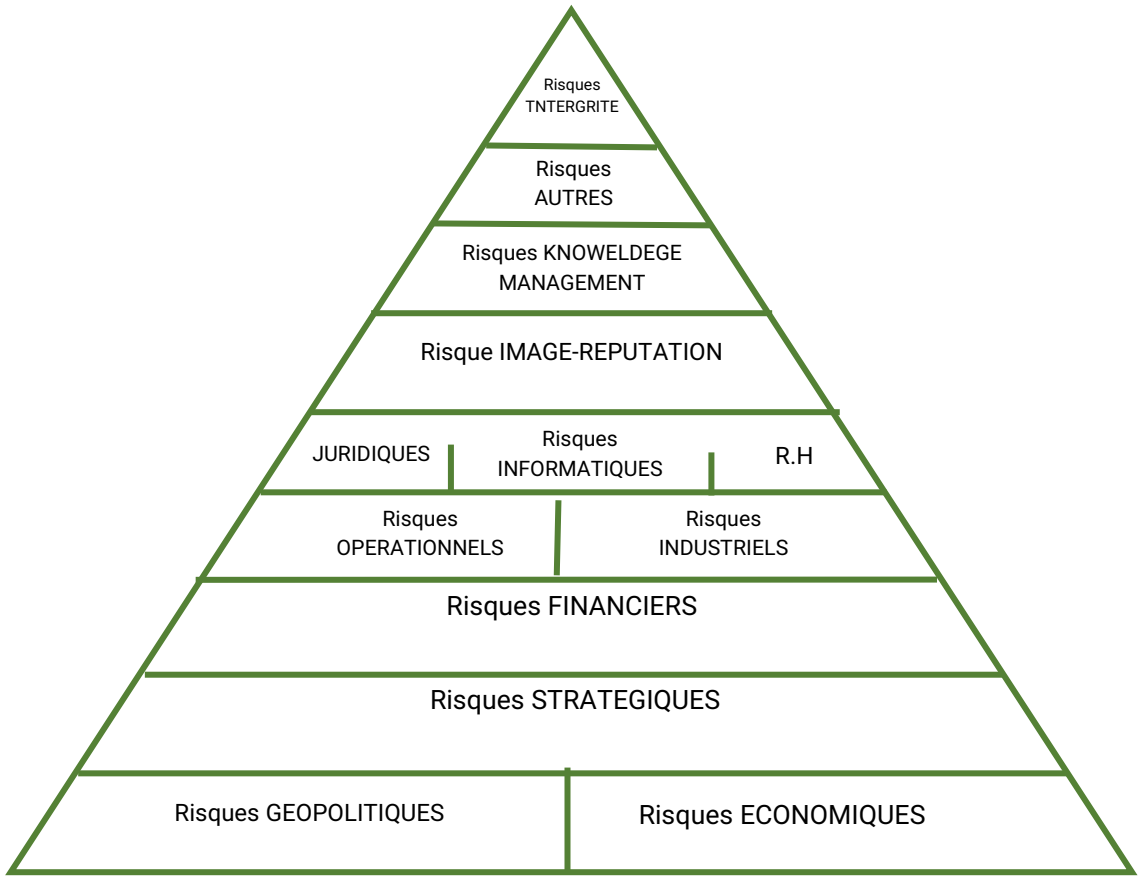


Figure (04) : Pyramide des risques. A partir de « La gestion des risques en entreprise ». De Darsa (2013a). p. 72. 3eme édition. France : Gereso.

- **Les risques géopolitiques :**

Il s'agit d'une manière fondamentale des risques liés directement ou indirectement à l'existence de l'entreprise à l'extérieur de ses frontières naturelles, c'est-à-dire lorsqu'elle exerce son activité à l'étranger, elle s'expose de quelque manière que ce soit à ces risques liés à ce(s) pays. Par exemple en Russie le risque lié à la faible exécution du droit commercial est important, tel que le risque qu'en gendre l'insécurité et la corruption élevée au Yémen, et cela au-delà des zones à risques grandement médiatisées comme l'Irak ou l'Afghanistan.

- **Les risques économiques :**

Ce sont ceux liés à l'économie dans laquelle l'entreprise évolue dans son ensemble, et plus précisément liés à l'inflation par exemple, le PIB ou encore la croissance des marchés sur lesquels l'entreprise se pose. Récemment, quelques risques économiques majeurs se sont concrétisés tel que l'évolution des cours du pétrole et de ses produits dérivés lors de la période 2007-2008 (un baril de 40$ est devenu de

145$ en 18mois).

- **Les risques stratégiques** :

Ils constituent les risques primordiaux à maitriser au sein de l'entreprise car ils sont ceux de défaillance d'un modèle stratégique de l'entreprise, en d'autres termes ce sont une incohérence entre l'analyse des besoins clients et le contenu d'une offre commerciale mis en œuvre. Parmi les nombreux cas de risque stratégique on peut citer l'exemple d'une croissance externe mal maitrisée ou une rupture technologique prise trop tôt …ou trop tard.

- **Les risques financiers :**

Il s'agit globalement d'une famille de risques composée des risques de liquidité, des risques de perte financière, des risques de taux d'intérêt, des risques de taux de change, des risques des marchés financiers, des risques comptables, des risques fiscaux, des risques de prise de contrôle, des risques fournisseur, des risques de sous-investissement, des risques de délinquance financière, des risques d'opportunité de délocalisation, des risques d'arrêt d'activité, des risques de structure des coûts, des risques de haut de bilan, des risques d'erreur d'investissement et enfin des risques de départ des actionnaires.

- **Les risques opérationnels :**

Ce sont les risques de perte résultant de défauts attribuables à des processus internes, des personnels ; des systèmes résultant d'événement extérieur. Ce sont aussi tous les risques pouvant engendrer un dommage ou une perte lors de la réalisation de l'activité courante de l'entreprise, dans ses cycles d'exploitation quotidiens. (L'objet central de notre mémoire)

- **Les risques industriels :**

Ce sont ceux spécifiquement engendrés par la mise en œuvre de processus industriels de production, on peut citer les risques de perte de qualité sur processus industriel ou de sur-qualité, les risques de rupture de chaine ou encore les risques environnementaux.

- **Les risques juridiques :**

Parmi les risques opérationnels on trouve les risques juridiques traités différemment compte tenu de leurs gravités. Ces risques concernent ceux qui peuvent impacter financièrement ou non, directement ou non l'entreprise à la suite d'une utilisation impropre d'un élément contractuel ou relationnel dans le cadre de ses activités économiques, potentiellement régis par la doctrine juridique.

- **Les risques informatiques :**

Autre catégorie majeure des risques opérationnels, et ils sont les risques de perte liés à la défaillance d'un ou plusieurs éléments matériels, physiques ou logiques constituant l'architecture, les outils, les données ou les applications informatiques de l'entreprise.

- **Les risque ressources humaines :**

Ce sont principalement les risque sociaux (climat social, gestion de la compétence…) et les risques psychosociaux (mal être, stress, suicide…), et c'est la dernière famille des risques opérationnels traités différemment.

- **Les risques d'image et de réputation :**

Il s'agit des risques liés à détérioration de l'image ou de la réputation de l'entreprise engendrant un dommage économique significatif.

- **Les risques de gestion de la connaissance :**

Appelés également risque de « Knowledge management », ils consistent à renforcer la pérennité de l'un des actifs essentiels de l'entreprise : ses connaissances et ses compétences.

- **Les autres risques :**

Tel que les risques de sur-qualité, ou ceux de défaillance du contrôle interne, ou encore les risques environnementaux nous ne pouvons pas tout citer, les risques de l'entreprise sont beaucoup trop nombreux.

- **Les risques d'intégrité :**

C'est le dernier risque qui, selon Darsa, est situé en haut de la pyramide des risques car l'intégrité individuelle constitue le risque ultime susceptible de remettre en cause la pérennité de l'entreprise.

1.4. Propriétés du risque

Toutes les règles internes ayant trait aux risques, s'imposent aux collaborateurs de l'entreprise, et décrivent les différents processus qui engagent l'entreprise, sont considérées comme gouvernance, à titre d'exemple la gouvernance sous-traitance qui est la réglementation interne de la mise en place de la sous-traitance d'un processus clé de l'entreprise.

Les gouvernances doivent être en adéquation avec la stratégie globale de l'entreprise et refléter fidèlement sa politique de risque. Elles sont élaborées par les directions

des risques et adoptées par l'organe d'administration de l'entreprise. Au cœur de la gestion du risque, l'entreprise doit imposer des gouvernances qui sont courtes, simples, lisibles et lues, car ces dernières sont l'infrastructure du dispositif, elles consolident des procédures complexes, évolutives, multirisques, multiprocessus, multi équipes et même parfois multi-pays. Leur cohérence, leur solidité et leur diffusion auprès de tous les collaborateurs sont les garants de la maîtrise globale des risques. (Dumora, 2017)

1.4.1. La culture du risque

C'est un élément clé, elle pousse à l'intégration de la gestion des risques dans le fonctionnement opérationnel de l'entreprise à son niveau le plus fin. Le risque ne peut être un domaine réservé à des équipes confinées et isolées, c'est pour cela qu'il est nécessaire pour l'efficacité du dispositif de risque, le partage de la culture du risque par l'ensemble des acteurs de l'entreprise. (Dumora, 2017)

1.4.2. Le cycle du risque

Il comporte 04 étapes majeures que Dumora (2017) a cité comme suit :

- **La politique de risque :** la première phase qui définit et met en place la politique du risque, elle explique la stratégie et la gestion du risque, les processus de décision.
- **La prise de risque** : la prise de risque recouvre la souscription d'affaires, l'acquisition de portefeuilles ou de compagnies mais également l'investissement dans des actifs financiers à l'égard des provisions techniques et la gestion tactique de ces actifs.
- **Le suivi des risques** : le suivi des risques intègre l'établissement de tous les états de reporting sur les risques, le calcul des provisions et de la solvabilité.
- **Le pilotage des risques** : Il s'agit de la mise en œuvre des transferts de risque (réassurance, titrisation, swaps de portefeuilles, etc…).

1.4.3. Coût du risque

Quels que soient les choix en matière de structuration du référentiel de risques, l'objectif est de les maitriser et de faciliter la classification et l'analyse agrégée des pertes. Pour Louisot (2005) le coût du risque est la raison pour laquelle il faut gérer le

risque.

Il ne s'agit pas d'un seul coût mais plutôt de cinq, à savoir les coûts administratifs liés au processus de gestion des risques, les coûts des efforts de réduction des risques, les coûts des instruments de financement des risques par transfert, les coûts des rétentions et les coûts des investissements abandonnés car excédant le seuil d'acceptabilité du risque de l'entreprise.

1.4.4. Appétit au risque

Le conseil d'administration établit ce qu'on l'appelle « l'appétence au risque », à laquelle le management souscrit en mettant en place des contrôles adaptés pour contenir le risque. L'appétit au risque est le niveau de risque maximum que l'entreprise est prête à accepter et à prendre dans le but d'accroître sa rentabilité, et d'atteindre ses objectifs stratégiques. (Brosse et Petsetidi Soupe, 2016)

1.4.5. Mesure du risque

Maurer (S. D.) défini la mesure du risque comme un capital réglementaire au titre du risque, qui doit couvrir à la fois les pertes attendues et les pertes exceptionnelles inattendues. Le Comité de Bâle propose trois approches distinctes pour déterminer ce capital :

- L'approche indicateur de base (Basic Indicator Approach ou BIA)
- L'approche standardisée (Standardised Approach ou SA)
- Les mesures dites avancées (Advanced Measurement Approach ou AMA).

2. La notion du risque opérationnel

Situés au cœur de la pyramide des risques, les risques opérationnels sont liés d'une manière générale à toute opération réalisée par une entreprise, ce qui rend la notion du risque opérationnel extrêmement large.

Souvent associés aux secteurs d'activité bancaire et d'assurance, le comité de Bâle II[1] (2004) en tant qu'ensemble de règles et de méthodes de calcul pour définir le niveau obligatoire de fonds propres sur risques, et dont la notion du risque opérationnel était une innovation. Il s'est basé sur l'aspect juridique pour définir les risques opérationnels comme les risques de pertes provenant de processus internes

[1] Les normes Bâle II constituent un dispositif prudentiel destiné à mieux appréhender les risques bancaires et principalement le risque de crédit ou de contrepartie et les exigences, pour garantir un niveau minimum de capitaux propres, afin d'assurer la solidarité financière.

inadéquats ou défaillants, de personnes et systèmes ou d'événements externes.

Jimenez et Merlier (2004) ont intégré dans leur ouvrage les définitions suivantes élargies du risque opérationnel « Tous les risques autres que les risques de crédit, les risques de marché et les risques financiers (taux de change, liquidité) » ou bien « Les risques opérationnels comprennent tous les risques de nature à interrompre ou compromettre le bon fonctionnement de l'entreprise, à remettre en cause l'atteinte de ses objectifs, ou à entraîner des dommages susceptibles d'affecter sa rentabilité ou son image ». (Pp.18)

Quant à l'Algérie, la définition du risque opérationnel est donnée par la règlementation n°2011-08 du 28 novembre 2011 relatif au contrôle interne des banques et établissements financiers :
« Le risque résultant d'une inadaptation ou d'une défaillance imputable à des procédures, personnels et systèmes internes ou à des évènements extérieurs. Il inclut les risques de fraude interne et externe » (p. 3). Cette définition peut être différente d'une banque à une autre selon son activité et son organisation interne.

De son côté Darsa (2013b) relie les RO à l'activité d'exploitation d'une entreprise.
C'est-à-dire que les RO viennent des différents processus et sous-processus liés à la mise en œuvre d'un cycle d'exploitation par une entreprise tel que la conception, le stockage ou le recrutement et la formation. Car ils viennent de la matérialisation des impacts directes ou indirectes engendrés par l'entreprise dans son activité quotidienne, donc dans son cycle d'exploitation. Il a aussi défini le RO comme étant un risque susceptible de dégrader la qualité des services ou des produits offerts au client et donc remettre en cause sa satisfaction.

De manière générale le risque opérationnel est le résultat des défaillances ou des dysfonctionnements des processus, du personnel, d'évènements et systèmes internes/externes à l'entreprise et qui rentrent dans son activité.

Ce risque peut engendrer des dommages et des coûts financiers plus ou moins graves. Il a donc, en plus de son impact interne lié au cycle d'exploitation et son impact externe lié à la satisfaction du client, un coût. D'où l'enjeu immense concernant sa couverture.

2.1. Composantes du RO

Le comité de Bâle II a adopté une approche causes-conséquences pour introduire les composantes du risque opérationnel en quatre sous-ensembles selon les défaillances qu'elles engendrent *:*

- **Une défaillance liée au système d'information :**

Elle est due au risque informatique engendré par un faible niveau de sécurité des systèmes informatiques. Ce risque se traduit par une défaillance matérielle au niveau

des moyens nécessaires à l'accomplissement des transactions habituelles et à l'exercice de l'activité, telle que des pannes informatiques résultant d'un acte de malveillance.

- **Une défaillance liée aux processus :**

Elle englobe le risque des processus qui est dû au non-respect des procédures et à la mauvaise gestion des processus, le risque d'interruption d'activité et d'interruption des systèmes, le risque comptable qui est dû à des informations erronées ou à une non application des normes comptables, et le risque de blanchiment qui consiste à participer directement ou indirectement à des opérations de blanchiment de sommes tirées de crimes ou de délit.

- **Une défaillance due aux personnes :**

Engendrée par le risque lié au processus qui est lui-même dû au facteur humain et dépend de la qualité du personnel, il provient de l'incompétence, manque de formation, vigilance, disponibilité… Ce risque englobe trois sous-risques à savoir le risque de fraude (les pertes dues à tout acte illégal caractérisé par la tromperie ou la dissimulation), le risque déontologique (le non-respect des règles de bonne conduite et de bonnes pratiques), et enfin le risque de mauvaise gestion du personnel (les pertes dues à des actes non conformes à la législation ou aux conventions relatives à l'emploi, la santé ou la sécurité).

- **Une défaillance due aux événements extérieurs :**

Générée par un risque lié aux événements extérieurs qui peut être à l'origine de risque politique ou de catastrophes naturelles. Encore une fois ce risque se compose de quatre sous-risques, le plus important c'est le risque juridique qui se définit comme une perte résultant de l'application imprévisible d'une loi ou d'une réglementation (risque de tout litige avec une contrepartie résultant de toutes imprécisions, lacunes, insuffisances susceptibles d'être imputables à l'établissement au titre de ses opérations).

Ensuite vient le risque réglementaire résultant de non-respect de la réglementation des assurances et le risque sur clients, produits et pratiques commerciales, qui est dû au manquement non institutionnel ou à la négligence à une obligation professionnelle envers les clients spécifiques, ou relative à la nature et conception d'un produit. Enfin le risque de dommages liés aux actifs corporels (la destruction des actifs physiques résultante d'une catastrophe naturelle).

2.2. Enjeux liés aux risques opérationnels

Avant de souligner les fondamentaux risques opérationnels présents dans une entreprise, Darsa (2013b) a jugé nécessaire de connaitre et de maitriser d'abord les cycles d'activités présent dans cette dernière étant donné que les RO viennent de l'activité de l'entreprise, en l'occurrence ces 4 grandes familles : infrastructure, exploitation, commerciale et support. L'objectif ici est de définir les enjeux qui concernes chaque famille en lien avec ses propres risques.

Pour les infrastructures il est important de veiller à la pérennité des actifs de la société afin d'assurer la continuité des services ainsi la satisfaction du client. De là on peut ressortir les différents enjeux tel que : l'accès (qui a accès à quoi ? quand ?), la sécurité des produits et services en assurant leur continuité, sécurisation des actifs logiques et virtuels (marques, brevets, réputation, nom).

L'identification des RO liés au cycle d'exploitation d'une entreprise nous permet non seulement de faire une liste non exhaustive des cycles d'exploitation, mais aussi de se rendre compte de la complexité des enjeux RO au sein des organisations. Parmi ces cycles on peut citer : approvisionnement et achats de matières première et marchandises dangereuse ou pas (comment assurer la pérennité de l'approvisionnement et éviter les ruptures ? et comment maitriser leur dangerosité ?), cycle de production (comment assurer une production continue en quantité et qualité tout le long du cycle d'exploitation ?) …

Les cycles commerciaux sont un gouffre de risques opérationnels en relation direct avec le client d'où ses enjeux. Par exemple le cycle d'écoute du marché et de veille concurrentielle doit être capable d'assurer l'évitement des risques à l'avenir pour l'entreprise grâce à la fiabilité de ses études. On peut aussi citer les cycles de gestion des relations clients qui expose l'entreprise directement au risque de perte si le client n'a pas été fidélisé…

Les risques opérationnels sont aussi quasi permanents dans les processus support de l'entreprise. Par exemple les processus administratives internes de l'entreprise doivent être capable de sécuriser leurs mécaniques de saisie comptable des opérations et de gestion des congés car ils peuvent avoir un impact direct ou non sur le client. On a aussi le cycle des enjeux qualité qui a pour mission de maitriser les outils de pilotage de l'entreprise et la qualité des services et produits offerts aux clients. On peut citer le cycle gestion de la connaissance ou bien celui de la gestion des archives…

A part ces quatre grandes familles, l'enjeu du RO s'élargie aussi à d'autres dimensions compte tenu de leurs interactions permanentes avec le processus d'exploitation de l'entreprise, ces dimensions sont : la sous-traitance et les activités externalisés, la fraude interne et externe, la conformité des opérations, et aussi toutes les opérations associées aux risques informatiques et juridiques et aussi humains…etc.

De là on peut constater que tout peut être considérer comme RO ou comme son

origine étant donné que ce dernier couvre tous les processus opérationnels, métiers, fonctionnels, organisationnels et d'exploitation de l'entreprise. Ce qui oblige toute organisation qui se respecte de bien définir, au-delà de l'enjeu, ce qui va être considérer comme risque opérationnel.

- **L'inventaire de l'existant :**

Cette démarche permet à l'entreprise de rédiger une liste exhaustive des multiples risques opérationnels présents en son sein (Darsa, 2013b), les étapes sont comme suit :

- Collecte de signes précurseurs sur l'existences de RO : réclamations, plaintes et remarques négatives des tiers, des clients, des fournisseurs ou des salariés.
- Audit interne et externe de l'entreprise : inspection des lieux et visites des fournisseurs et clients…
- Collecte des incidents et dysfonctionnements ayant engendré un coût du risque : pertes liées à une mauvaise gestion, à un défaut perçu par un client…
- Cartographie des processus opérationnels de l'entreprise : par service (qui fait quoi, quand et comment ?), par processus et sous-processus, et par mode opératoire (work-flows et schéma des flux).
- Qualification du niveau de criticité des processus et sous-processus de l'entreprise en maitrisant les RO présents dans l'entreprise.

Une fois cet inventaire terminé, l'entreprise se retrouvera confronter à une multitude de risque qui, au premier abord, peuvent tout être des RO, et pour définir ce qui est opérationnel ou pas, elle doit d'abord déterminer le degré de mesure de l'enjeu pour chaque risque au cas par cas afin de délimiter le rayon des RO en écartant ceux qui ne le sont pas et non le contraire. Cette délimitation des enjeux permet aussi de réduire le coût du risque opérationnel dans l'entreprise.

Enfin, c'est uniquement après la maitrise de la notion du risque opérationnel qu'on pourra rentrer en détail dans l'étude des différentes composantes et typologies de ce risque dans le but de bien les maîtriser.

2.3. Typologies du risque opérationnel

En 1999, THAI Nguyen Hong a été le premier à réaliser une classification des risques opérationnel en deux typologies à savoir les risques de dysfonctionnement et les risques de manipulation frauduleuse. (Raïs H. M, 2012)

Bale II a continué en classant les risques opérationnels sur sept catégories : fraude interne impliquant au moins un membre de l'entreprise, fraude externe, insuffisance des pratiques internes concernant les ressources humaines et la sécurité du lieu de travail, clients, produits et pratiques commerciales : manquement, délibéré ou non, à une obligation professionnelle envers un client, à la nature ou aux caractéristiques

d'un produit. Dommages aux actifs physiques, interruption d'activité et dysfonctionnement des systèmes, dysfonctionnement des processus de traitement-exécution, passation d'ordre, livraison, gestion des processus intégrant les relations avec les contreparties commerciales et les fournisseurs. (Caclin F,2021).

Un groupe de travail de l'IFACI, Institut Français d'Audit et de Contrôle Internes a, quant à lui, élaboré une nomenclature des risques pour les entreprises d'assurance. Le référentiel proposé est constitué de trois niveaux : (Optimind, 2011)

- Le premier niveau concerne les grandes familles de risques, dont le risque opérationnel.

- Le deuxième niveau précise la catégorie de risque dans laquelle on se situe au sein d'une même famille : production, humain, commercial, organisation, système d'information, logistique hors SI ou relation avec les tiers.

- Le troisième niveau offre un degré de détail supplémentaire au sein de ces catégories.

Une autre classification des risques basée sur deux critères (Desroches et all,2005) :

- **En fonction de leur évolution :** les risques à effets convergents dont la gravité diminue avec le temps ou à effets divergents dont la gravité augmente avec le temps.

- **En fonction de leur impact** : les risques à effets directs et indirects ou en cascades induisant un enchainement de différentes natures.

2.3.1. Les sept catégories de RO

L'IA (Institut Des Actuaires Français, 2016) a dressé une typologie du RO comportant trois niveaux : le 1er est équivalent aux 7 catégories de Bâle 3, ce qui leur a permis de regrouper les risques sur des catégories équivalentes. Le 2eme niveau contient des catégories plus détaillées et fait apparaître des spécificités du secteur de l'assurance. Le dernier niveau comporte une liste non-exhaustive des exemples de risques avec leur classement.

Catégorie événement (Niveau 1)		Définition
1	**Fraude interne.**	Pertes causées par des auteurs internes à l'entreprise : salariés, stagiaires, conjoins ou amis des salariés motivés par différents objectifs tel que le vol, la dégradation et le détournement des actifs qui touchent tous types d'entreprisse, de la TPE à la multinationale. C'est donc un RO puissant à ne pas négliger.
2	**Fraude externe.**	Pertes causées par tiers : hackeurs, pirates, acteurs du banditismes motivés par le détournement d'image et la contrefaçon qui rentrent dans une guerre économique contre l'entreprise. Un RO à ne pas négliger au même titre que la fraude interne.
3	**Pratiques en matière d'emploi et sécurité sur le lieu de travail.**	Pertes résultant d'actes non conformes à la législation relatives à l'emploi, la santé ou la sécurité de la part d'un tiers.
4	**Clients, produits et pratiques commerciales.**	Pertes résultant d'une négligence professionnelle envers des clients spécifiques ou résultant de la nature ou de la conception d'un produit.
5	**Dommages aux actifs corporels.**	Destruction ou dommages résultant d'une catastrophe naturelle ou d'un sinistre.
6	**Interruptions d'activité et dysfonctionnements des systèmes.**	Pertes résultant de dysfonctionnement de l'activité ou des systèmes.
7	**Exécution, livraison et gestion des processus.**	Pertes résultant d'un problème dans le traitement d'une transaction ou dans la gestion des processus ou de relations avec les contreparties commerciales et fournisseurs.

Tableau (4) : classement des risques opérationnels inspiré de « Le risque opérationnel, un nouveau challenge pour l'actuaire ». Institut des Actuaires. (2016). P.15. https://www.institutdesactuaires.com/global/gene/link.php?doc_id=9761&fg=1

En reprenant la définition du risque opérationnel précédemment cité nous pouvons constater que tous les risques sont des risques opérationnels en puissance, c'est pour cela que Darsa (2013b) a jugé nécessaire de traiter les risques juridiques, informatiques et ressources humaines séparément due à leur liaison au cycle d'exploitation de l'organisation, donc ils sont des RO à part entières.

2.3.2. Les risques juridiques

La question du risque juridique a été souvent négligé et sous-traité par les dirigeants, car à première vue sa relation avec les cycles d'exploitation est éloignée par rapport aux autres risques opérationnels. Ce qui n'est plus le cas aujourd'hui, compte tenu de leur diversité et de l'impact négative qu'ils peuvent avoir sur l'organisation.

Un risque juridique est un risque pouvant impacter financièrement ou non, directement ou non l'entreprise, à la suite d'une utilisation ou d'une application impropre d'un ou plusieurs éléments contractuels ou relationnels dans le cadre de ses activités économiques, potentiellement régis par la doctrine juridique ou les us et coutumes en vigueur. (Darsa, 2013b, p.148)

De multiples causes peuvent être à l'origine de ces risques, par exemple au niveau contractuel :

- Qualité et intégrité des contrats clients, fournisseurs, distributeur, de franchise, de prestations critiques et externalisées ;
- Qualité et intégrité des contrats d'assurance, de baux (locaux), et des contrats de travail.

Au niveau de la conformité des processus opérationnels mis en œuvre avec la loi au sens large, les principales sources de risques juridiques peuvent concernés, une fois les processus de l'entreprise identifies :

- Le respect/maitrise ou non du droit du consommateur, commercial, de la concurrence, du droit pénal et des marques ;
- Le respect/maitrise ou non du code de la propriété intellectuelle, monétaire et financier, du code du travail, des marchés publics ;
- Le respect/maitrise de la législation comptable, financière, fiscale et sociale…

Une autre source de risques juridiques à ne pas négliger concerne les contentieux, c'est-à-dire les risques associés aux recouvrements des créances clients qui viennent :

- Des litiges commerciales ou techniques, des comportements commerciaux inadaptés ;
- Situations d'insolvabilités inadaptés et défaillance financière du débiteur ;
- Processus d'identification du risque client non performent…

2.3.2.1. Le risque pénal

Un risque juridique particulier à ne pas négliger vu la croissance actuelle de la pénalisation du monde des affaires et les risques encourus par les dirigeants et l'entreprise en général s'il n'est pas bien identifié et maitrisé.

Parmi les infractions relatives au risque pénal dans l'entreprise on peut citer les abus de confiance et de biens sociaux, contrefaçon de logiciels, financement du terrorisme, atteinte à la vie privée, banqueroute, usurpation d'identité, discrimination et harcèlement moral…

2.3.3. Le risque informatique

Moins négligé que le risque juridique, la maitrise du risque informatique occupe une place primordiale dans la stratégie de l'entreprise afin de s'assurer la pérennité opérationnelle de l'organisation et de limiter son coût.

Le risque informatique ou risque des technologies de l'information et de la communication TIC, ou risque du système d'information correspond au risque de perte résultant d'une organisation inadéquate, d'un défaut de fonctionnement, ou d'une insuffisante sécurité du système d'information, entendu comme l'ensemble des équipements systèmes et réseaux et des moyens humains destinés au traitement de l'information de l'institution. » ACPR Banque De France.

2.3.3.1. Causes, conséquences et impacte financier

La survenance de risque informatique peut engendrer des coûts financiers variables, selon la gravité et la difficulté de la gestion du risque. De perte de productivités et/ou de remplacement, et avoir des impacts sur l'image client/fournisseur et sur la fiabilité des outils IT. Ceci due à l'indisponibilité

temporaire ou non d'applications, de serveurs réseaux ou de matériels tel que le serveur web, de perte d'exploitation, et aussi d'handicape opérationnelles des équipes techniques qui se retrouvent sans outils…etc. (Darsa, 2013b)

Parmi les causes de ces risques on peut citer : les panne d'infrastructures, de matériels ou de logiciels, attaque virale et violation volontaire ou involontaire de la sécurité physique (vol, incendie…), Potentiel machines insuffisant…

2.3.3.2. Appréhension du risque informatique

Etant un risque majeur, technique, et source d'innovation, de différenciation de valeurs pour l'entreprise. Une gestion rapide, efficace et à jour de ce dernier s'impose. Pour se faire, plusieurs approches d'identifications s'offrent à nous, les unes plus pertinentes que les autres et présentés sous forme de check-lists d'enjeux et de points à prendre en considération : (Darsa, 2013b)

- **L'approche général :** constitue une première liste de risque à considérer qui est orienté métier et qui s'articule autour des grands axes fonctionnels et organisationnels de l'entreprise.
- **L'approche « menaces » :** pour d'identifier les risques liés à l'infrastructure informatique, elle comporte 18 points.
- **L'approche synthétique :** complémentaire de la précédente, elle contient les risques informatiques présents dans chaque entreprise, ils sont du nombre de 27.
- **L'approche IT (informatique) :** qui constitue une liste exhaustive de 99 enjeux liés à la maitrise opérationnel du risque informatique.
- **L'approche projet ou « risque projet » :** la non maîtrise d'un projet informatique engendre divers risques informatiques qu'il faut considérer pour en réduire le risque projet et le coût qu'il engendre. Une liste de 79 risques projets est proposée pour amorcer tout projet informatique.

Compte tenu des enjeux et de la diversité des risque informatiques, l'entreprise doit réfléchir à mettre en œuvre une stratégie de sécurité efficace pour identifier au mieux les zones à risques.

Pour se faire, Darsa (2013b) nous propose de confronter toutes les approches d'identification des risques informatiques afin de nous assurer l'identification d'un maximum des zones à risque non identifiable par l'application d'une seule approche. Ce qu'il appelle **« théorie du frottement »,** son but est de permettre à chaque entreprise de formuler sa propre méthodologie et liste de risques approprié à son

activité et son environnement.

Quel-que-soit la ou les approches utilisées, l'objectif fondamental est de réduire le coût du risque informatique associées aux enjeux opérationnels en définissant la méthodologie adaptée selon les objectifs stratégiques de l'organisation.

2.3.4. Risques sociaux et psychosociaux

Dernière famille des risques opérationnels traitée de manière spécifique, les risques « ressources humaines » sont constitués de deux grandes familles de risques distinctes, à savoir les risques « sociaux » qui sont liés à la gestion des ressources humaines d'une entreprise, et les risques « psychosociaux » relatifs à l'individu lui-même.

- **Risques sociaux :**

Les risques appelés sociaux d'une entreprise proviennent de trois dimensions fortement liées, et chacune d'entre elles représente un risque qui lui est attaché. Le climat social en est la première dimension, la qualité de ce climat peut engendrer des risques tel que voir émerger et perdurer un mouvement social, ou bien toute action de salariés détériorant l'activité de l'organisation. Ces risques sont présents également en cas d'existence de conflits latents entre la direction et ses salariés ou autre. (Darsa, 2013b)

La deuxième dimension est celle du (Turn-over) ou bien de la rotation des collaborateurs (les équipes constitutives des entreprises) suite à un départ non souhaité d'un d'entre eux.

Le Turn-over peut se manifester sur plusieurs niveaux, en engendrant des risques sur chacun, il existe donc des Turn-over des équipes opérationnelles, des équipes d'encadrement (middle management) ou celui des équipes de direction (comité de direction, comité exécutif).
On peut illustrer ça par le cas de perte d'un « homme clé », dont le départ impacte lourdement et durablement l'entreprise, le Turn-over lié à cette perte peut générer des risques importants tel que la perte de compétence et l'incapacité de la remplacer…etc.

La dernière dimension est liée essentiellement au respect des droits et des obligations sociales de l'entreprise vis-à-vis de ses salariés, elle cause des risques appelés sociaux « techniques » que les dirigeants doivent être extrêmement vigilants à leur égard. (Darsa)

Parmi les principaux risques sociaux techniques à identifier et à maitriser, le respect des obligations sociales de tout employeurs vis-à-vis de ses salariés tel que le droit à la formation et les obligations associées à la médecine du travail ou encore aux contraintes de type Environnement Hygiène Sécurité.

- **Risques psychosociaux :**

Risque social à part entière, le risque psychosocial relève, quant à lui, de l'individu lui-même, quel que soit sa fonction ou son positionnement dans l'entreprise. (Darsa, 2013b)

Les risques fondamentaux à prendre en considération sont, le stress ou toutes formes de mal-être ou de souffrance du collaborateur ou de l'encadrant, les risques ou les conduites suicidaires des salariés ou des dirigeants, tous types d'agression physique ou verbale entre collaborateurs et responsables ou autres, le risque d'enlèvement, de séquestration ou d'assassinat des collaborateurs ou dirigeants ainsi que toutes formes d'harcèlent moral.

Les risques psychosociaux sont tellement variés qu'il est parfois difficile de les identifier et les appréhender pour l'encadrant, en prenant compte de la difficulté à connaitre la situation réelle des équipes et de leurs états d'esprit.

Afin de faire face aux risque sociaux et psychosociaux, la communication est primordiale, ainsi que d'échanger avec les salariés et les encadrants, écouter leurs plaintes et leurs réclamations et ne jamais accepter une situation intolérable. (Darsa)

2.4. Facteurs de développements des RO

Récemment, la perception du risque opérationnel a changé car il est devenu de plus en plus important, et cela sous l'effet de principaux facteurs qui ont contribué d'une façon ou d'une autre à son développement à travers le temps : (Darsa, 2013b)

2.4.1. Fonctionnement des marchés

La globalisation des marchés et des produits a contribué à accroître la concurrence entre les établissements ainsi que leurs domaines d'intervention et par conséquent les risques associés. Les évolutions technologiques à leur tour permettant une banalisation de la gestion des opérations en temps réel, ont donné naissance à de nouveaux risques tel que le risques de règlement, le risques de fraude interne ou externe et la défaillances techniques et humaines.

2.4.2. Sophistication des techniques financières

Les nouvelles techniques financières sont de plus en plus complexes à gérer et rendent certains risques plus présents. Par exemple, le développement du commerce électronique soulève de nouvelles questions en matière de fraude ou de sécurité informatique, alors que les montages financiers, de plus en plus élaborés,

exposent les établissements à un risque juridique accru.

2.4.3. Evolution des processus internes

L'automatisation croissante du fonctionnement interne grâce aux outils informatiques, engendre des risques de nature technique, et le recours à l'externalisation de certaines activités contribue à l'accroissement des risques opérationnels.

2.4.4. Evénements extérieurs

Les risques exceptionnels ont une faible occurrence et une forte intensité, tel que les catastrophes naturelles par exemple, malgré qu'ils ne soient pas nouveaux, mais leur perception est aujourd'hui beaucoup plus forte qu'auparavant. Ils font ainsi l'objet d'une attention accrue.

3. Organisation du contrôle du RO

La présence des risques sur tous les niveaux et sur toutes les fonctions de l'entreprise, engendre de nombreux acteurs dans l'organisation d'un dispositif de maitrise des risques opérationnels, et dans les périodes de crises, ces acteurs doivent optimiser la création de valeur et cela grâce à une organisation efficiente. (Merlier et Jimenez, 2004)

Dans le cas où l'organisation défini bien les responsabilités, les missions et les domaines d'interaction des acteurs, leurs objectifs peuvent être atteints.

La démarche d'organisation exige que les dirigeants s'engagent dans une politique de maitrise des risques efficace en prenant compte l'importance de la transparence à tous les niveaux de l'entreprise, y compris les plus élevés. Afin de parvenir à une organisation efficace et efficiente il est primordial de définir à chaque fonction les responsabilités associées.

Tout organisme doit intégrer une vision étendue du contrôle des risques afin de garantir leur pérennité, sécuriser leurs activités et prémunir leur patrimoine et pour cela, ils doivent aussi
développer cette culture où chacun participe à limiter et à anticiper le risque. (Merlier et Jimenez)

3.1. Le rôle de la DG dans le contrôle des RO

Pour Merlier et Jimenez (2004), la direction générale possède un rôle fondamental et elle doit être impliquée fortement dans la mise en place d'un dispositif de gestion des risques opérationnels, car c'est elle qui valide la politique de risque et les allocations de couverture de ce dernier. Elle permet également la mise en place du dispositif avec maitrise et dans des délais précis.

Devant les autorités de contrôle, la direction générale assume la réalité et l'efficacité du dispositif, et cela en assurant quatre (4) responsabilités, à savoir :

- La responsabilité du système de gestion et de maitrise des risques et de son implémentation ;
- La responsabilité de la stratégie de couverture des risques opérationnels et l'acceptation des risques résiduels ;
- La responsabilité de l'allocation des fonds propres nécessaires à la couverture des risques ;
- La responsabilité d'assurer la réalisation d'un audit régulier du système en toute indépendance pour vérifier l'exhaustivité et la qualité du système de contrôle mis en œuvre.

3.2. La direction des RO et les lignes métiers

La direction des risques opérationnels est le principal outil d'assurance de l'efficacité du processus que la direction générale possède, et pour lui permettre une vision transversale qui favorise la prévention au traitement ponctuel, cette dernière nécessite une indépendance des fonctions opérationnelles. (Merlier et Jimenez, 2004)

3.2.1. Les missions de la direction des RO

Merlier et Jimenez (2004) définissent les missions de la direction des risques opérationnels comme suit :

- La définition des politiques et procédures pour la gestion des risques opérationnels ;
- La coordination des travaux réalisés dans les lignes métiers ;
- La validation des modèles les plus appropriés et leur mis en œuvre ;
- La définition des outils transversaux de mesure et de suivi (le système d'information) ;
- La consolidation des données et la préparation des arbitrages de la direction générale ;

- L'analyse des remontées d'informations des lignes opérationnelles et le contrôle du bon traitement de l'ensemble des incidents ;
- Une intervention directe dans certains dossiers à fort impact en aide aux opérationnels, en particulier pour éviter des absences de traitement qui sont un facteur aggravant ;
- La participation à la validation des états réglementaires.

3.2.2. Les lignes métiers et les opérationnels

La politique de maîtrise des risques a plusieurs enjeux, et le plus remarquable est celui de la formation et de la mobilisation des équipes aux risques existants et à la bonne gestion des incidents. Dans le dispositif, on trouve souvent trois (03) niveaux de fonctions opérationnelles qui auront une responsabilité différente chacune. (Merlier et Jimenez, 2004)

Le premier niveau est celui de la direction de la fonction opérationnelle qui a parmi ses taches l'assurance de la mise en place de la politique des risques, la décision des mesures prioritaires et la fixation des plannings et la veille à la formation des personnels et à l'actualisation du dispositif.

Le management est le second niveau, car parmi ses responsabilités, il assure la mise en place d'outils d'évaluation et de reporting dans le domaine de compétence concernée, il assure aussi la validation des informations sur les incidents, le traitement de ces derniers, la transparence du dispositif…

Le troisième niveau consiste aux opérationnels qui gèrent les processus et la production de l'établissement, qui assurent aussi la détection et l'enregistrement des incidents, la mise en place des mesures correctives et conservatoires à leur niveau et ils proposent des plans d'action pour la correction des incidents.

3.3. La relation entre les RO et les lignes transverses

Les métiers transverses sont en général en charge de risques particuliers et ont des contraintes spécifiques qui impliquent des traitements parfois particuliers. Lorsque ce n'est pas le cas, une fonction transverse est soumise à un dispositif similaire à celui mis-en place pour une fonction opérationnelle classique. (Merlier et Jimenez, 2004)

3.3.1. Les systèmes d'information

L'intervention des personnes en charge du SI est importante lorsqu'il y a une mise en place d'un SI propre aux besoins des risques opérationnels, elles contribuent également à la maitrise de ces derniers. En général, on trouve une direction des SI

(DSI) et un RSSI (responsable de la sécurité des SI) qui ont la responsabilité des risques associés au SI.

Quelle que soit l'organisation retenue pour ces fonctions, elles ont un rôle majeur à jouer dans le dispositif de maitrise des risques opérationnels et ce à tous les niveaux de l'entreprise.
Dans cette relation, deux caractéristiques se dégagent souvent, à savoir une réelle culture de prévention des risques et une certaine opacité du système. (Merlier et Jimenez, 2004)

3.3.2. Les ressources humaines

Ils vont avoir un accès privilégié à tous les risques qui vont concerner les collaborateurs de l'entreprise, que ce soit individuellement ou collectivement. Avec cette fonction, il est nécessaire de définir comment intégrer dans le dispositif de mesure des risques opérationnels des événements ponctuels qui auront une influence sur les risques portés.

Les accidents de travail, les fraudes ou encore les vols sont considérés tel des risques individuels, et la principale problématique est celle de protéger les données nominatives, c'est-à-dire que seules les personnes habilitées auront droit d'avoir connaissance aux informations concernant les personnes en cause. (Merlier et Jimenez, 2004)

Quant aux autres risques liés aux RH, ils sont relatifs à l'inadéquation des compétences par rapport aux missions, au turn-over des équipes, aux personnes sensibles pour une activité…etc.

3.3.3. La logistique

Notamment celles relatives à la sécurité des biens et des personnes, elles sont souvent assurées par des personnes dédiées qui ont des compétences en matière de gestion d'immeubles, de sécurité d'incendie, de gestion des accès, de négociations auprès des fournisseurs…etc. dans le cas où ces fonctions seraient largement décentralisées dans les métiers opérationnels, le schéma traditionnel déjà exposé sera maintenu avec si possible la sensibilisation particulière des personnes en charge de ces domaines. (Merlier et Jimenez, 2004)

3.3.4. Les services juridiques

Ces services sont bien formés aux risques spécifiques dont ils ont la responsabilité et jouent souvent un rôle de prévention important, mais ils ne sont pas tentés de dissimuler des informations qui pourraient mettre en cause leur responsabilité car ils ne sont pas à l'origine des dossiers contentieux. La relation avec le suivi des risques opérationnels se fait donc assez naturellement, et elle ne doit pas poser de problèmes particuliers. (Merlier et Jimenez, 2004)

3.4. La relation entre les RO et la direction de l'audit interne

La direction de l'audit interne est souvent considérée comme le garant de la réalité et de la matérialité du système de contrôle interne. Elle assure par ses missions régulières d'inspection, un contrôle de la mise en œuvre de la politique de la direction générale en matière de sécurité, de respect des règles internes et de la réglementation.

Cette fonction nécessite une complète indépendance afin d'assurer son objectivité, elle ne doit donc pas avoir d'implication dans la définition et la mise en œuvre des politiques et outils de maitrise des risques opérationnels.

Son rôle majeur dans le dispositif sera de valider la pertinence et la qualité du système du système de maitrise des risques et de proposer des mesures d'amélioration.

3.4.1. Le RO et le contrôle interne

La mise en œuvre des mesures du contrôle interne a pour but d'assurer une certaine maitrise des risques, et ce grâce à un processus de gestion de risques opérationnels intégré visant à améliorer l'efficience d'une entreprise. Le contrôle interne doit inclure un système de contrôle des opérations et des procédures internes, une organisation comptable, des systèmes de mesure des risques et des résultats, des systèmes de surveillance et de maitrise des risques, un système de documentation et de traitement de l'information, et enfin un dispositif de surveillance des flux d'espèces et de titres. (Merlier et Jimenez, 2004)

Le dispositif de maitrise des risques opérationnels complète activement ces grands principes en permettant une mesure de certains risques qui étaient jusqu'alors peu ou mal appréhendés. Cela mène les risques opérationnels à être intégrés dans la démarche globale de contrôle interne.

Section 3 : la gestion des risques des systèmes d'information

La sécurité des systèmes d'information est maintenant abordée par des approches basées sur les risques. Car ceci permet de réduire considérablement les pertes liées aux faiblesses de sécurité des systèmes d'information. L'évolution du métier de Risk manager, qui s'intéresse à la sécurité du SI, permet de mieux appréhender la gestion des risques SI.

1. La fonction gestion des risques d'un SI

La gestion des risques est définie par l'ISO/IEC comme un ensemble d'activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque (Guide 73, 2009).
Sa finalité est de :

- Améliorer la sécurisation des systèmes d'information.
- Justifier le budget alloué à la sécurisation du système d'information.
- Prouver la crédibilité du système d'information à l'aide des analyses effectuées.

Il faut noter que le principal objectif de la gestion des risques d'un SI est d'assurer la sécurité de ce système en adaptant de mode de gestion selon le risque estimé.

La gestion des risques dépend d'un comité appelé Team Risk Management (TRM) qui a pour rôle l'identification et l'évaluation d'un risque dans le but de déterminer la meilleure réponse possible. L'approche du TRM est basée sur quatre catégories de risques : le risque stratégique, le risque opérationnel, le risque lié aux projets, le risque de litige. (Guide 73 : 2009)

1.1. Avantages de la gestion des risques SI

- Aide les organisations à prendre des décisions rationnelles sur la sécurité de leur SI ;
- La gouvernance du risque du SI permet de protéger la technologie et l'infrastructure physique de ces systèmes, ce qui favorise la croissance de l'activité et la création de valeur ;
- Freiner la détérioration et l'utilisation anormale des systèmes et réseaux ;
- Détecter toute atteinte à l'intégrité, la disponibilité et la confidentialité des informations, d'en limiter les conséquences et le cas échéant, poursuivre l'auteur du délit.

Les travaux de Westerman et Hunter démontrent qu'une association efficace des volets de gestion du risque ; processus de gouvernance, assise informatique, culture de prise en compte des risques. Permet d'avoir une meilleur performance opérationnelle informatique et métier, et d'en tirer plusieurs avantages : (Ikkou et Elouidani 2016).

- Faire face aux sensibilisations insuffisantes et aux manques de personnels formés ou d'outils pour la gestion du risque ;
- Meilleures performances informatiques dans la prévention des incidents, l'accompagnement de l'évolution de l'entreprise, et la mise en adéquation des objectifs informatiques et métier grâce à une équipe informatique efficace ;
- Eviter les risques financiers y afférents tel que : perte de réputation, réduction de la valeur des actions, perte de ventes, de productivité et d'avantages compétitifs…

1.2. Le top 10 des risques opérationnels lié aux SI

Une étude appelée CBOK (Common Body Of Knowledge) a été mené par l'IIA en 2015 dans le but de mettre en évidence les dix principaux risques SI grâce à des entretiens avec des responsables de l'audit interne et des experts en SI du monde entier. L'ordre de priorité de ces risques peut varier selon le secteur d'activité.

1.2.1. Cybersécurité

Jugé comme étant le plus significatif à 82 % par les experts SI, le vol, par intrusion, d'informations sensibles ou confidentielles est très pris au sérieux par les dirigeants, les auditeurs internes et les administrateurs, vue les conséquences qu'une telle fuite de données pourrait avoir sur l'image de marque et la réputation.

1.2.2. Protection des données

La protection des données, en matière de confidentialité, d'intégrité et d'accès, était avant assuré par des dispositifs tels que des pares-feux, des systèmes de prévention et de détection des intrusions, des outils de filtrage des contenus ou des mécanismes de surveillance du réseau. Une protection à un seul niveau qui n'était pas vraiment efficace. C'est pourquoi on opte désormais pour une protection à plusieurs niveaux piloté par le responsable de la sécurité des systèmes d'information, et comprend systématiquement les éléments suivants :

- Un solide processus d'évaluation des risques ;
- Des politiques efficaces de gouvernance et de conformité ;
- Des règles et des normes formalisées et diffusées ;
- Un plan de sensibilisation et de formation efficace ;
- Des procédures efficientes de contrôle des accès ;
- Des plans de reprise et de continuité d'activité après sinistres ;
- Des processus de gestion des actifs, du réseau, des patchs et du changement fonctionnels ;
- Des mesures strictes en matière de sécurité physique.

1.2.3. Les projets SI

Toutes les organisations ont besoin de mettre à jour leurs systèmes d'information. Le coût très élevé lié aux défaillances logicielles explique pourquoi un large budget SI est consacré aux projets. Malheureusement, les chances de réussite sont faibles. Les risques liés aux projets SI sont généralement :

- Non-respect des échéances et du budget ;

- Logiciels défaillants car non testés avant leur déploiement ;
- Moindre efficience et intégration par rapport au plan initial ;
- Fonctionnalités moindres par rapport au business case indiqué dans le projet approuvé ;
- Le manque de leadership constitue un autre problème majeur car il peut nuire au projet à plusieurs niveaux, surtout par rapport à la gestion du risque.

1.2.4. Gouvernance des SI

La gouvernance des SI comprend la direction, les structures organisationnelles et les processus qui garantissent que les technologies de l'information soutiennent la stratégie et les objectifs de l'organisation. (IIA/IFACI 2013)

Compte tenu des sommes dépensées pour les SI et de leurs impacts sur les clients et les opérations. La gouvernance des SI devrait être en mesure d'assurer la performance de ces derniers dans la maîtrise des risques et la saisie des opportunités de progression.

Pour être efficace, tout programme de gouvernance des SI doit, au minimum :

- Être explicitement aligné sur les besoins métiers ;
- Créer une valeur mesurable pour les métiers ;
- Prévoir des dispositifs de contrôle et de devoir de rendre compte des ressources, des risques, des performances et des coûts.

1.2.5. Prestation informatique externalisé

L'externalisation peut exposer l'organisation à des risques susceptibles de rester inconnus jusqu'à ce qu'une défaillance survienne. Pour les éviter, les responsables doivent s'assurer que le contrat initial couvre les aspects suivants : supervision, surveillance, audit, sécurité physique et logique, dotation en personnel approprié, interlocuteur clé, accès à l'information, plans de continuité d'activité /reprise après sinistre, contrats de niveau de service, et reporting.

1.2.6. Utilisation des réseaux sociaux

La rapidité de diffusion des communications via les réseaux sociaux a contraint les organisations à définir des règles et procédures en la matière pour éviter les risques suivants :

- Poursuites judiciaires pour diffamation, harcèlement, atteinte à la vie privée, etc. ;
- Fuites d'informations exclusives ou de secrets commerciaux, susceptibles d'avoir une incidence sur la compétitivité ;
- Atteintes à la réputation de l'organisation du fait de communications calomnieuses, désobligeantes ou imprudentes.

Pour faire face aux risques liés aux réseaux sociaux, les organisations doivent intégrer les étapes suivantes dans leurs procédures :

- Définir une politique d'utilisation des réseaux sociaux appropriée pour l'organisation, la diffuser dans un programme de sécurité, et la mettre en œuvre grâce au déploiement d'un logiciel de filtrage des contenus dédié aux SI ;
- Surveiller les résultats afin de s'assurer que cette politique est bien appliquée ;
- Sanctionner les infractions à cette politique.

1.2.7. Informatique mobile

L'information se déplace avec l'utilisateur. Les données des appareils mobiles doivent donc faire l'objet de mesures de sécurité aussi robustes que celles des Sièges de ces organisations.

La puissance informatique actuelle et la disponibilité de la connectivité Internet partout où il existe une connexion Wi-Fi ou cellulaire, ont entraîné l'apparition d'une multitude de risques liés aux différents dispositifs et configurations réseau. Cette situation remet en cause les approches de gestion des risques traditionnellement adoptées par les DSI.

- **Risques liés à la sécurité** : la perte ou le vol d'appareils contentant des données personnelles ou propres à l'organisation, sont facilement compromis surtout si les dispositifs de contrôle de sécurité ne sont pas

efficaces ;

- **Risques liés à la conformité** : Avec l'introduction de la politique « Apportez vos outils personnels » (Bring Your Own Device, ou BYOD), les organisations comptent beaucoup sur les utilisateurs pour respecter les règles et procédures applicables, alors que ces dernières peuvent les contourner en trouvent comme excuse la haute fréquence des mises à jour par exemple ;

- **Risques liés à la protection de la vie privée** : La politique BYOD peut soulever des pré- occupations en matière de protection de la vie privée du point de vue de l'organisation et des collaborateurs ;

- **Risques liés à la gestion de la flotte d'appareils** : Par exemple, en cas de mise à niveau, l'obligation de se débarrasser de l'ancien appareil peut accroître les risques liés à la gestion, sachant qu'ils contiennent des données de l'organisation. Il est donc nécessaire d'assurer une gestion des supports SI efficace ;

- **Risques juridiques** : Les conséquences juridiques liées au stockage des données de l'organisation sur des appareils intelligents doivent être pris en considération.

1.2.8. Compétences des auditeurs internes en matière de SI

D'après Mark Salamasick, directeur du département Audit de l'Université du Texas, plusieurs raisons justifient le nombre faible d'auditeurs compétents en SI. La plus courante étant que les professionnels des SI ont la possibilité d'être exposés à des technologies plus novatrices et d'exiger une rémunération plus élevée que celle des auditeurs SI.

Certaines organisations forment en interne leur auditeurs financiers et opérationnels au SI, mais ils ne sont pas au final accrédités par la DSI et le management.

1.2.9. Technologies émergentes

L'évolution des SI génère de nouveaux risques pour l'organisation. Les technologies émergentes peuvent avoir diverses conséquences selon les

organisations après leur déploiement (big data, impression 3D, robotique…) c'est dans le secteur financier que le niveau de risque inhérent concernant la fiabilité du Big Data est perçu comme le plus élevé.

1.2.10. Sensibilisation du conseil eu du comité d'audit aux enjeux SI

Les SI constituent un atout majeur pour l'organisation et requièrent un fort investissement. Il est donc risqué pour le Conseil de posséder une expertise limitée en la matière. Il devrait acquérir les compétences nécessaires pour être en mesure de demander des précisions sur la performance des SI au DSI. Tout comme il s'est doté de solides compétences financières au fil des années.

1.3. Méthodes de gestion des risques SI

La complexité de la notion du risque et la multitude de normes et modèles dédier à la gestion du risque ; plus de 200 méthodes de gestion/analyse des risques sont déclinées actuellement à travers le monde, n'aident pas les organisations à choisir laquelle est adapté à leur activité. (Mayer et Humbert, 2006).

La bonne connaissance et compréhension des fondements caractérisant les concepts et processus de la gestion des risques pour les SI préalablement établi, aiderait à faire un choix optimal concernant la méthode à adopter pour la gestion des risques SI.

Mayer et Humbert, (2006) ont dégagés dans leur étude les méthodes les plus utilisées dans ce domaine à savoir :

1.3.1. EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)

Créée en 1995 par la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information), elle se compose de cinq guides (Introduction, Démarche, Techniques, Outillages pour l'appréciation des risques et Outillages pour le traitement des risques) et d'un logiciel support. Etant gratuite, la méthode travaille en prenant compte du contexte de l'organisation cible, en privilégiant le périmètre du SI, les éléments essentiels, les fonctions et les informations, et enfin les entités.

Dans un second plan, elle permet de dégager les besoins via une grille des services souhaités de sécurité (respect des critères de confidentialité, intégrité et disponibilité). Puis, en se basant sur les normes ISO 15408,1 7799, EBIOS prépare les contres mesures adaptés aux besoins de l'organisation selon le risque identifié.

Certains considèrent que EBIOS est qu'une méthodologie d'analyse des risques car elle ne prend pas en considération toutes les étapes du processus de gestion du

risque.

1.3.2. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

Publiée par le Software Engineering Institute (SEI) de la Carnegie Mellon University, reconnue dans le domaine de la sécurité des SI (fédération des Computer Emergency & Response Team CERTS). Elle se caractérise par son utilisation des ressources uniquement internes à l'organisation pour analyser les risques qui pèsent sur ses actifs opérationnels et mesurer et les vulnérabilités pesant sur eux, en respectant trois phases :

- **La phase 1 (vue organisationnelle)** : elle permet d'identifier les ressources informatiques importantes, les menaces associées et les exigences de sécurité qui leur sont associées.
- **La phase 2 (vue technique)** : elle permet d'identifier les vulnérabilités de l'infrastructure (ces dernières, une fois couplées aux menaces, créant le risque).
- **La phase 3 :** elle décline le développement de la stratégie de sécurité et sa planification (protection et plan de réduction des risques).

OCTAVE a la même critiquer que EBIOS car elle aussi n'aborde pas les deux dernières étapes du processus de gestion du risque.

1.3.3. MEHARI (Méthode Harmonisé D'analyse Des Risques)

Maintenue en France par le CLUSIF (Club de la Sécurité des Systèmes d'Information Français), MEHARI, dérivée de deux autres méthodes d'analyse des risques (MARION et MELISA), est l'une des méthodes d 'analyse des risques les plus utilisées actuellement. Composée de plusieurs modules, elle appréhende le risque de différentes manières au sein d'une organisation et elle permet :

- D'analyser les enjeux de la sécurité et de classifier les ressources et informations selon la confidentialité, l'intégrité et la disponibilité ;
- D'auditer les services de sécurité, afin d'en tirer leurs points forts et faibles ;
- D'analyser les situations de risques, évaluer leurs impacts, les facteurs d'atténuation, puis déduire un indicateur de gravité du risque.

Cette démarche se décline au niveau stratégique, mais aussi opérationnel. Le premier niveau permet la cohérence des besoins et du contexte de l'ensemble de

l'organisation. Le second niveau définit les unités business autonomes au cœur de l'organisation et en charge des décisions nécessaires en matière de sécurité.

En se basant sur l'audit de sécurité, MEHARI réalise facilement des plans d'actions à entreprendre pour faire face aux faiblesses relevées. La même chose pour la gestion des risques de projets, en tenant compte de la sécurité en se basant sur l'analyse des risques, un plan d'action directement intégré au projet, est facilement élaboré, ce qui facilite la gestion du projet.

Cette méthode s'aligne avec les deux premières en termes de couverture du processus de gestion des risques.

2. Référentiels normatifs liés à la gestion des risques SI

Dans le cadre du management des risques, les référentiels sont nécessaires pour uniformiser les pratiques surtout, en ce qui concerne les processus de management des risques. Ce domaine comporte plusieurs référentiels, le plus anciens d'entre eux est l'Australien/New Zealand Standards 4360. Approuvé par ISO, il comporte deux parties, la synthèse du standard du Risk Management et le Risk Management guidelines-Compagnon, il met l'accent sur l'importance de l'intégration de la culture du risque dans l'organisation. (Dale F Cooper, 2007)

On peut aussi citer le modèle Criteria on Contrôle Committee « COCO » qui est un référentiel canadien, et aussi le Turnbul guidance du Royaume-Uni, le référentiel européen au nom de la Fédération of European Risk Management « FERMA » qui est un recueil et un cadre des meilleurs pratiques européennes sur la gestion des risques… mais dans ce point nous allons présenter les référentiels les plus utilisés.

2.1. COSO et COSO-ERM

Le Committee Of Sponsoring Organization est le premier référentiel ou Framework de gestion des risques en entreprise qui a publié son premier document COSO en 1992.
Créé par la National Commission On Fraudulent Financial Reporting (Treadway Commission) qui a vu le jour en 1985 grâce à la collaboration de cinq grandes associations professionnels américaines (AAA, AICPA, FEI, IIA, IMA) alimentées par la volonté de lutter contre la fraude et la corruption, surtout après les scandales financiers des années 1970 aux Etats Unis d'Amérique. Ces évènements ont poussé à réfléchir à la création d'un cadre commun de control interne aux entreprises jusqu'à là défini que par les normes d'audit interne de l'AICPA. (Schick et all, 2010)

En 2004, un second document COSO 2 est créé. Celui-ci est axé d'avantage sur le processus de management des risques en réponse d'une part, à l'évolution risquée du contexte économique qui pousse les entreprises à se munir de ce processus de maitrise des risques et d'autre part, de la volonté de renforcer la gouvernance de

l'entreprise entre surveillance et transparence des comités et dirigeants en réponse aux scandales précédemment cité. (Schick et all)

Appelé aussi COSO ERM « Enterprise Risk Management », il définit le management des risques comme étant :

Le management des risques est 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-ERM, 2004, p. 3)

Son objectif est d'aider le manager à réduire le risque de résultats négatifs et à augmenter les avantages relatifs à la stratégie et à l'exploitation quotidienne de l'entreprise dans le but de créer de la valeur ajoutée pour toutes les parties prenantes. Et ceci en lui permettant de faire face efficacement aux incertitudes et aux évènements futures.

Une mise à jour du COSO ERM est parue en 2013, elle comporte les évolutions des environnements opérationnelles et les attentes accrus du control interne, et elle est motivé par :

- L'émergence de risques nouveaux et la vulnérabilité des systèmes d'informations surtout en ce qui concerne la cybercriminalité ;
- La responsabilisation du personnel et le maitrise des risques par la gouvernance ;
- L'efficacité du control interne résultant de l'articulation entre opérationnels, fonctions support et audit interne.

Ce cadre définit les composants essentiels, suggère un langage commun et fournit une orientation et des conseils clairs pour la gestion des risques d'entreprise.

Etant donné que le management des risques est un processus multidirectionnel et répétitif par lequel n'importe quel élément a une influence immédiate et directe sur

les autres, COSO ERM met en relation les objectifs d'une organisation et les éléments du dispositif de management des risques qui représentent ce qui est nécessaire à leur réalisation. (IFACI, 2017)

La relation est illustrée par une matrice en trois dimensions ayant la forme d'un cube qui illustre la façon d'appréhender le management des risques dans sa globalité.

Les quatre grandes catégories d'objectifs stratégiques, opérationnels, reporting et conformité sont représentées par les colonnes. Les huit éléments du management des risques par les lignes, et les unités de l'organisation par la troisième dimension.

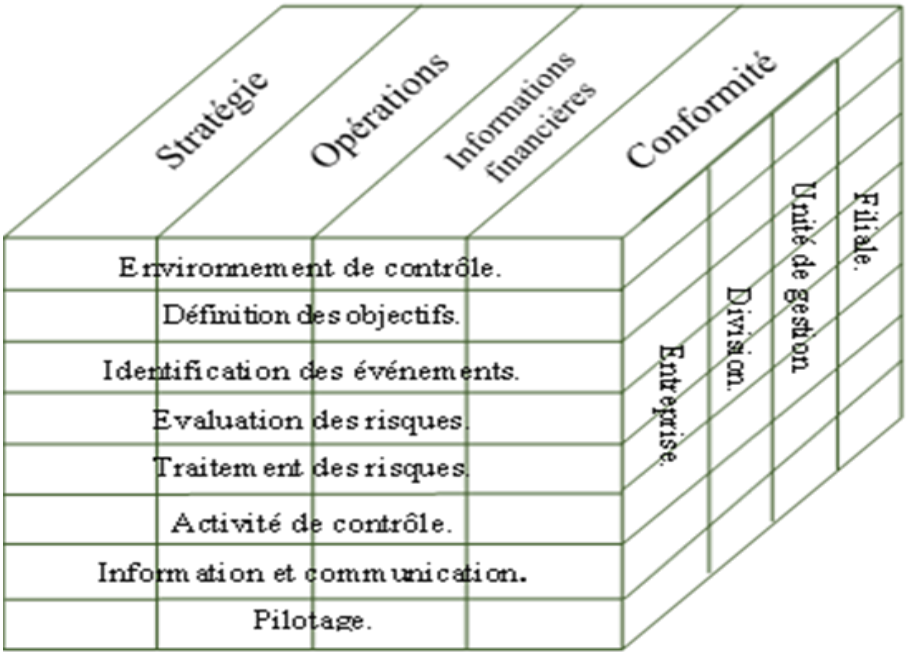


Figure (05) : cube COSO à partir de « Le management des risques de l'entreprise, Cadre de Référence. Synthèse », IFACI, 2017, p. 5.

2.2. CobiT (Control Objectives for Information and Related Technology)

Publié en 1996, le CobiT est une méthodologie d'évaluation des services informatiques au sein de l'organisation. Il propose un ensemble de bonnes pratiques de gouvernance IT. Le CobiT propose au management un cadre de référence des pratiques de contrôle et de maîtrise de l'informatique, applicable pour évaluer un environnement informatique existant ou en phase d'implémentation. (Ferchichi A. 2008).

Ses processus concernent les domaines fonctionnels que sont : planification et organisation, acquisition et mise en place, distribution et support, et surveillance et

évaluation.

Dans son guide de mise en œuvre, le CobiT propose également des outils d'analyse et d'évaluation de risques des environnements informatisés. Les trente-quatre (34) processus du CobiT permettent de couvrir trois cent dix-huit (318) objectifs. (Moisand et Garnier De Labareyre, 2009).

L'utilisation du CobiT permet aux systèmes d'information de l'entreprise :

- De s'aligner sur le métier de l'entreprise ;
- D'apporter un plus aux métiers ;
- De gérer au mieux ses ressources ;
- De gérer les risques de façon efficace.

Le CobiT est l'élément de base pour une bonne gouvernance d'activité et institutionnelle de l'entreprise. La mise en œuvre de ses bonnes pratiques crée de la valeur ajoutée. Il aborde la gouvernance de la sécurité de l'information en s'intéressant à : (Moisand et Garnier De Labareyre, 2009).

- La prise en compte de la sécurité de l'information dans l'alignement stratégique ;
- La prise de mesures appropriées pour limiter les risques et leurs conséquences potentielles à un niveau acceptable ;
- La connaissance et la protection des actifs ;
- La gestion des ressources ;
- La mesure pour s'assurer que les objectifs de sécurité sont bien atteints ;
- L'apport de valeur par l'optimisation des investissements en matière de sécurité de l'information ;
- Les bénéfices retirés ;
- L'intégration de la sécurité de l'information dans les processus.

Globalement, CobiT aborde la sécurité de l'information dans plus de vingt processus

sur trente-quatre. Mais les processus suivants font apparaître une dimension sécurité importante dans les objectifs de contrôle :

- Faire connaître les buts et orientations du management ;
- Évaluer et gérer les risques ;
- Assurer un service continu
- Assurer la sécurité des systèmes.

2.3. La norme ISO 31000 (Management Du Risque)

Modifié en 2018, la norme internationale pour le management des risques, ISO 31000 est élaborée par le comité technique ISO/TC 262 appartenant à l'organisation internationale de normalisation « ISO ». Adressée à quiconque souhaite gérer les risques, cette norme est compatible avec tout organisme, quels que soit son type, sa taille, son activité et son emplacement. (ISO 31000, 2018)

L'ISO 31000 fournit des principes, des lignes directrices générales sur le management des risques, et un processus applicable pour toute organisme souhaitant augmenter ses chances d'atteindre ses objectifs, mieux cerner les opportunités et les menaces, et d'allouer les ressources pour le management du risque de manière efficace.

Elle rappelle aussi que l'intérêt et l'objectif du management des risques réside dans la globalité de son application sur tous les domaines de l'organisation. (ISO 31000, 2018)

Cette norme aide les organismes à développer une stratégie de management du risque visant à identifier et à atténuer les risques de façon efficace. Ces organismes sont ainsi plus susceptibles d'atteindre leurs objectifs et disposent d'actifs mieux protégés. (SÉGOT et al, 2011)

Son objectif premier c'est de contribuer au développement d'une culture du management du risque permettant aux employés et aux parties prenantes de prendre conscience de l'importance du suivi et de la gestion des risques.

La mise en œuvre d'ISO 31000 permet également aux organismes de comprendre les opportunités positives et les conséquences négatives associées au risque et les aide à prendre des décisions plus éclairées, et ainsi plus efficaces, notamment en matière d'affectation des ressources. Cette norme peut en outre jouer un rôle essentiel dans l'amélioration de la gouvernance d'un organisme et, à terme, de sa performance. (SÉGOT et al, 2011)

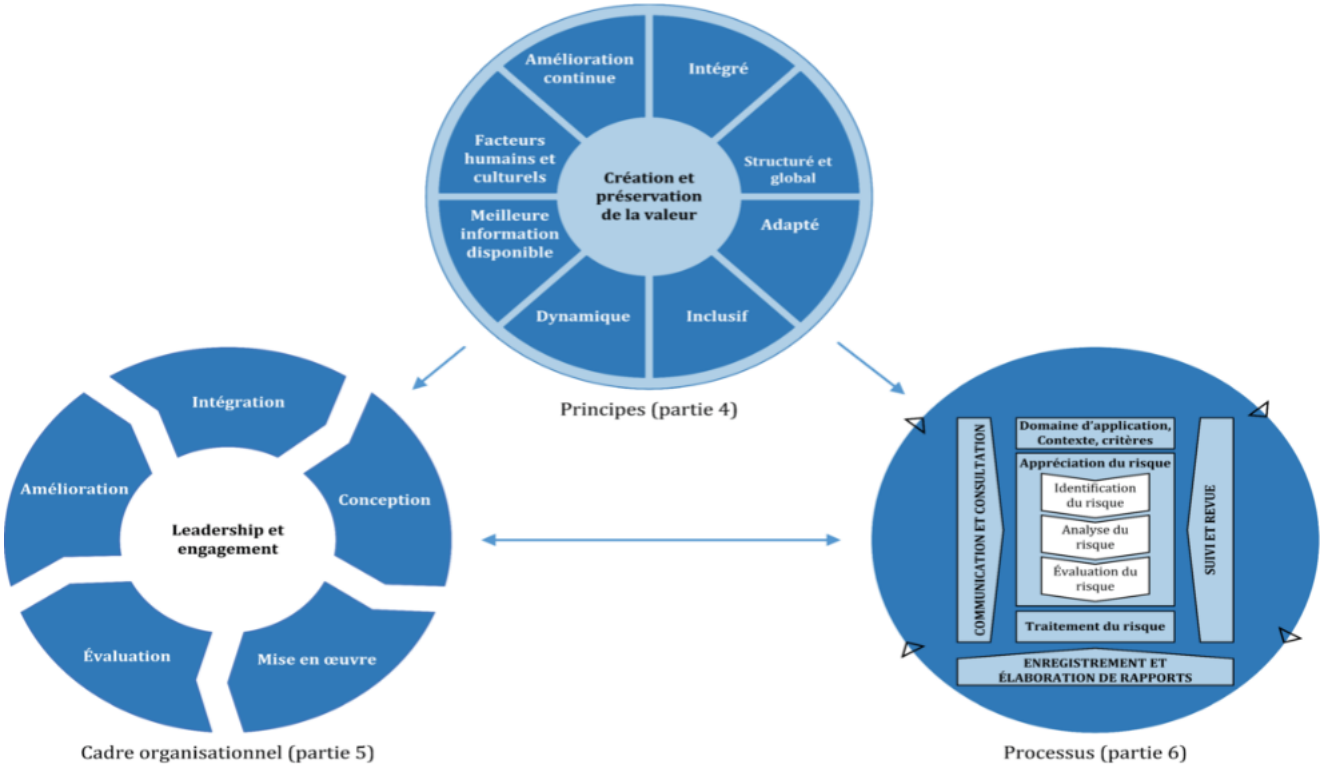


Figure (06) : Principes, cadre organisationnel et processus de la norme ISO 31000 à partir de « ISO 31000 : 2018, Management du Risque, lignes directrices.
https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:fr

3. Rôle de la DSI dans la gestion des risques SI

La Direction des Systèmes Informatique et/ou d'Information correspond à l'unité chargée de la stratégie IT et des systèmes informatiques nécessaires au soutien des objectifs de l'entreprise. Au milieu des années 80, le rôle de la DSI était essentiellement technique.

A mesure que le stockage, la transmission et l'analyse d'informations électroniques gagnaient en importance, la DSI a été perçue comme un contributeur clé dans la formulation des objectifs stratégiques. Elle doit sensibiliser les cadres de direction, ainsi que les employés, à la valeur ajoutée des systèmes informatiques et aux risques qu'ils induisent pour l'entreprise.

Conséquence de responsabilités stratégiques croissantes, les DSI des grandes entreprises se composent des équipes de spécialistes destinées à gérer des domaines spécifiques de l'informatique. (Thevenot 2011)

La DSI est généralement organisée autour de 3 pôles de compétences : Études, Expertise et Production, supportés par des fonctions administratives (RH, Contrôle de gestion, etc…) et pilotés par un comité directeur. Ces trois pôles de compétences sont composés des fonctions suivantes :

- **Le pilotage de la DSI** : Aligner le SI aux exigences de la direction générale et déterminer les orientations stratégiques de la DSI.
- **L'assistance utilisateurs** : Le point de contact quotidien avec les utilisateurs, qui assure le support lié au SI.
- **Fonctions transverses** : Les fonctions garantissant le bon déroulement de la gestion du SI, à savoir le pilotage des projets et leur adéquation avec ce qui a été arbitré par le comité directeur, définition des normes et méthodes à appliquer au sein de la DSI, etc.
- **La relation fournisseurs** : Assurer la relation avec les fournisseurs,
- Études : Toutes les fonctions autour de la conception du SI (Build) permettant de construire et faire évoluer le SI dans un contexte projets,
- **Production & Infrastructures** : Toutes les fonctions liées à la production du SI reposant sur des machines et serveurs,
- **Expertise** : L'ensemble des experts qui apportent leur savoir-faire sur les projets, le support ou encore les évolutions du SI,
- **Fonctions support** : Les fonctions administratives transverses à la DSI, et les entités veillant à la mise en place des processus et référentiels liés au fonctionnement général de la DSI

Le risque est partie intégrante de la vie des entreprises. La gestion du risque, généralement considérée comme une activité de support avec quelques nuances en fonction du secteur d'activité, se prévoit en amont et implique aussi le département informatique.

Mais pour quel rôle ?

Si l'entreprise décide de prendre des risques, elle doit aussi s'assurer qu'ils ne la mettent pas en péril. Un accident industriel, un fournisseur qui fait défaut ou une attaque numérique qui bloque tout le système d'information sont des événements ni rares ni marginaux.

En y ajoutant les évolutions réglementaires ou législatives qui changent dans le temps et diffèrent d'un pays à l'autre, on prend la pleine mesure de l'exposition au risque, active ou passive, à laquelle l'entreprise doit faire face avec une vigilance accrue. En matière de gestion des risques la DSI a un rôle d'autant plus primordial à jouer.

Afin d'éviter de se retrouver démuni lorsqu'un événement ou une crise survient, il est nécessaire de préparer en amont, d'anticiper la gestion des risques, de voir les crises, et de veiller en permanence à la mise en conformité de l'entreprise, et c'est à quoi sert le dispositif de continuité d'activité.

Le plan de continuité doit englober toute la chaîne de valeur pour assurer la cohérence des actions prévues, car l'entreprise n'est pas seule dans son environnement, elle fait partie d'un écosystème qui doit être intégré à son plan de continuité.

Dans les grands groupes, appréhender le plan de continuité comme partie intégrante du dispositif de gestion de risque et de conformité est par conséquent un programme complexe, polymorphe, et incombant le plus souvent au département de gestion du risque.

Il engage généralement une cartographie des risques, afin de les répertorier, de les évaluer et d'analyser leur impact business, puis prévoit la mise en place de dispositifs de prévention, de contrôle et d'intervention. Le gestionnaire de risque n'est pas seul dans sa mission car la direction des systèmes d'information (DSI) est partenaire et son support indispensables.

D'abord, en raison-même de la digitalisation de l'activité, le risque technologique est devenu un risque opérationnel également couvert par un plan de continuité. Que ce soit pour la détection des fraudes, le déni de service, le piratage, la cybercriminalité… etc.

Les gestionnaires de risque peuvent s'appuyer sur l'historique et les compétences des DSI.
Mais les risques inhérents à la fonction informatique cohabitent avec ceux d'autres départements et ces derniers reposent aussi sur une forme d'automatisation à base de composants informatiques.

Un premier exemple est porté par les dispositifs de Scoring crédit dans les banques, automatisés depuis bien longtemps à base de moteurs d'inférence. Un autre sur les dispositifs « Bâlois » répondant aux exigences la réglementation « Bâle II ou Bâle III », qui calculent automatiquement le capital à réserver pour couvrir les risques de crédit, de marché et les risques opérationnels, à partir de méthodes statistiques simples ou avancées.

Un troisième exemple nous est apporté par les dispositifs de gestion de crise, qui

nous ramènent au cœur-même des dispositifs de continuité d'activité.

Le rôle de la DSI est critique pour la gestion des risques et la continuité à l'ère digitale car cette dernière apporte des outils et des méthodes permettant de cartographier toutes les natures de risques en les liant directement à la connaissance de l'entreprise et de ses actifs, qu'ils soient métiers, informatiques ou humains.

En conclusion, si la DSI est aussi importante pour la gestion du risque et la continuité d'activité c'est qu'il est impossible aujourd'hui d'envisager la gouvernance d'une organisation à l'ère digitale sans en confier une part significative à la DSI. Ceci peut commencer par la gestion automatisée des indicateurs de performance, pour aboutir à ce que l'on pourrait appeler une cybernétique de la gestion du risque, où, une fois décantées les priorités, quels sont les processus critiques et les ressources, donc critiques, sur lesquels ils reposent, la fonction informatique est mise à contribution pour automatiser autant que possible, et améliorer ensuite, le contrôle des risques.

Conclusion

L'information est l'une des ressources majeures de l'entreprise, au même niveau que les ressources liées à la production. C'est pour ça que la gestion des risques lié aux technologies de l'information et aux systèmes d'information doit avoir une place importante dans la starie de l'organisation qu'elle-que soit sont type.

Entre les risques liés à l'activité et les risques liés à la technologie, la panoplie des risques liés aux Systèmes d'Information est très large. C'est pourquoi il faut dédier à chacun d'eux une attention particulière surtout en ce qui concerne les risques opérationnels.

La gestion des risques opérationnels liés aux Systèmes d'Information, leur évaluation et la mesure de leurs coûts, est bénéfique pour l'organisation car elle assure l'optimisation des ressources consacrées à la sécurité, et permet de mieux contrôler les conséquences négatives des RO, mais aussi de créer de nouvelles sources d'opportunités pour l'entreprise. Le risque devient alors un actif et une source de profits pour l'entreprise.

Pour réussir à gérer les risques liés aux technologies de l'information, et plus particulièrement les risques opérationnels des SI, il est important de responsabiliser les managers dans l'identification, l'évaluation et la mise en œuvre de processus appropriés en ce qui concerne la protection des données et la sécurité de l'information. Ils doivent comprendre qu'il existe des coûts associés à différents types de risques.

En outre, en appliquant une gestion active des risques, les organisations qui utilisent des technologies de l'information sont plus capable d'assumer la responsabilité des risques qu'elles peuvent rencontrer ou produire. En d'autres termes, cela leur permet d'être conscients des risques liés aux SI auxquels ils sont confrontés.

CHAPITRE 2 :
Enterprise Risk Management et la fonction d'audit

Introduction

Pour l'IIA, l'Entreprise Risk Management est un processus structuré, cohérent et continu, appliqué à l'ensemble de l'organisation, qui permet d'identifier et d'évaluer les risques, ainsi que de décider des réponses à apporter aux opportunités et menaces qui affectent la réalisation des objectifs, et d'en rendre compte.

L'Entreprise Risk Management est un processus primordial dans toute société, à lui seul il constitue la principale approche de gestion et d'optimisation des risques, permettant à une organisation de déterminer le degré d'incertitude et de risque acceptable.

Parmi tous les référentiels normatifs relatifs à la gestion des risques, nous avons choisis, dans la première section de présenter la norme ISO 31000 « Risk Management », car cette dernière, dans sa version de 2018 présente un processus ERM complet, détaillé et applicables à tous types d'entreprises.

Dans un second temps, nous allons parler du contrôle interne en tant qu'ensemble de processus visant à apporter un degré raisonnable de confiance quant à la réalisation des objectifs. Ainsi que la place qu'il occupe dans le dispositif de gouvernance et de gestion des risques, et la relation qui le lie avec le processus ERM.

Puis nous tenterons de clarifier le rôle et les missions des auditeurs internes dans le management des risques, tout en soulignant les rôles spécifiques du management des risques qui, selon les normes de l'IIA, ne doivent pas être assumés par les auditeurs internes.

La fin de ce chapitre va nous permettre de savoir si l'implication correcte des auditeurs internes dans l'ERM et son évaluation, aidera l'organisme à améliorer ce processus et à optimiser sa performance.

Section 1 : Le processus de management des risques « ERM » selon l'ISO 31000

En plus du cadre organisationnel et du pilotage continue, le processus de management des risques « Entreprise Risk Mangement » est l'une des composantes du dispositif global de la gestion des risques. Mis en place et adapté par les entreprises pour faire face aux différents risques qu'elle rencontre.

1. Le concept ERM

Face aux risques qui surgissent, l'entreprise emploi tout un processus de management des risques qui implique une application systématique de politiques, de procédures et de pratiques aux activités de communication et de consultation, d'établissement du contexte et d'appréciation, de traitement, de suivi, de revue, d'enregistrement et de compte rendu du risque. (ISO 31000, 2018)

Le processus de management des risques est une méthode clairement défini pour comprendre quels risques et opportunités sont présents, comment ils peuvent impacter un projet ou une organisation et comment y répondre. L'ERM est la principale approche de gestion et d'optimisation des risques, permettant à une organisation de déterminer le degré d'incertitude et de risque acceptable pour une organisation. (Gregory Kigen s. d.)

Afin que le processus de management des risques soit mis-en place de manière efficace, il est nécessaire d'avoir un appui et un soutien du directeur général, une prise en toute considération de la valeur ajoutée qu'apportera ce processus au profit de l'organisation, une coopération des managers fonctionnels et opérationnels, une fiabilité des informations, et une objectivité dans l'identification et l'évaluation des risques.

Mais surtout dans un premier temps une fixation des objectifs est obligatoire pour que la gestion des risques puisse identifier les évènements potentiels pouvant en affecter la réalisation. En outre, elle permet de s'assurer de la bonne mise en place d'un processus de fixation de ces objectifs. (CORDEL, 2013)

1.1. Objectifs et avantages

Les objectifs visés par le processus de management des risques sont divers, principalement ils concernent le gain de rentabilité et de productivité, la gestion des coûts et des délais, la qualité d'un produit et ce en analysant et gérant l'ensemble des risques et en proposant et coordonnant la mise en place des plans d'actions. Il constitue clairement un outil d'aide à la prise de décision pour les responsables de l'entreprise. Mandzila et Zéghal (2009).

Le guide d'audit IFACI (2003) énonce les principaux objectifs d'un processus de management des risques suivants :

- Identification et hiérarchisation rapide des risques auxquels l'organisation peut faire face ;
- Recenser de la façon la plus exhaustive possible les risques majeurs susceptibles d'affecter l'organisation, et ce en les décrivant avec précision selon leur impact et leur probabilité d'occurrence grâce à une élaboration de cartographie de ces risques.
- Détermination d'un niveau de risques acceptable pour l'organisation, donc une limite ou un seuil auquel dépasser mettrai en danger l'organisation ;
- Définition et mise en œuvre de mesures d'atténuation et de maîtrise des risques compte tenu des seuils jugés acceptables ;
- Suivi permanent des activités afin de réévaluer périodiquement les risques et l'efficacité des contrôles et d'assurer une cohérence globale de la méthode de gestion des risques d'une activité à l'autre ;
- Information périodique du Conseil et de la direction générale sur les résultats des processus de management des risques ;
- Maintien d'un niveau de qualité des reporting interne et externe ;
- Alimenter le plan d'audit interne ;
- Perfectionner le système de communication entre toutes les parties concernées en élaborant un dispositif commun sur la politique de risque adaptée par l'organisation.

De manière générale, le processus de management des risques offre l'avantage de promouvoir ou renforcer une culture de risque au sein de l'entreprise et de partager les meilleures pratiques en apportant des outils et des méthodes aux managers pour les aider à identifier, évaluer et traiter leurs risques. D'autres avantages sont à citer tel que (IFACI) :

- La mise en place d'un pilotage intégré des risques ;
- Attirer l'attention de toutes les parties de l'organisation sur l'importance de tous les risques quel que soit son ampleur (faible moyenne ou forte) ;

- Instaurer un langage commun sur les risques au sein de l'organisation ;
- Mobiliser l'ensemble des intervenants et fournir l'occasion de mettre en place une gestion coordonnée des risques ;
- Satisfaire aux exigences de transparence concernant les risques…

1.2. Limites

DUMORA (2017), affirme que le dispositif de management des risques doit être complet pour couvrir l'ensemble des risques auxquels l'entreprise est exposée, cohérent pour réconcilier dans une vision globale la stratégie de risque des actionnaires, des managers et les prises de décisions opérationnelles de l'ensemble des collaborateurs de l'entreprise. Le dispositif doit être homogène car il est inutile de surprotéger l'entreprise face à un risque pour l'exposer de manière inconsidérée à un autre, il doit être également intégré dans l'activité opérationnelle car il ne s'agit pas d'une organisation parallèle réservée à quelques fonctions spécifiques de l'entreprise mais d'un cadre opérationnel pour tous les collaborateurs. Enfin le dispositif doit être simple et compréhensible, ce ne doit pas être un processus administratif complexe mais un système d'information et des procédures de décision faciles à appréhender par les acteurs de l'entreprise.

Il existe des limites liées au processus de management des risques malgré son importance. CORDEL (2013) les a présentées principalement dans la définition des objectifs, comme suit :

- Une réconciliation difficile entre les objectifs de l'entreprise qui sont ceux assignés aux individus chargés de les mettre en œuvre et les objectifs de ces derniers.
- Des objectifs stratégiques, opérationnels, ou de conformité souffrant de contradictions
- Des objectifs simplement irréalistes, au regard des moyens qui sont donnés
- Une communication d'objectif parfois défaillante
- Lorsque l'objectif est autosuffisant et que sa réalisation n'a pas vraiment de sens

- Lorsque l'objectif n'est pas quantifiable, donc il n'est pas possible de mesurer le degré d'atteinte d'objectifs

Des limites sont aussi observables quant à la cartographie des risques :

- La problématique de compression des intervalles, qui se traduit par le fait que les risques ayant de différents degrés de probabilité se retrouvent dans la même catégorie seulement parce que les deux sont inférieurs au seuil attribué à cette catégorie (un risque à 1% de chance de se produire et un autre à 15% sont considérés les deux à occurrence faible parce qu'ils sont inférieurs à 20%)
- Dans les échelles utilisées pour établir les cartographies, il existe des présomptions d'intervalles réguliers
- La problématique de la corrélation des risques due à la présupposition qu'ils sont indépendants.

1.3. Outils

Il existe plusieurs outils de gestion des risques, et leur utilisation dépend de la diversité des projets (CORDEL, 2013), voici quelques-uns :

- **Les contrôles :**

Le dispositif de contrôle interne des risques est transversal par rapport à l'ensemble des filières de risque. Il s'appuie sur trois niveaux, un premier concernant les contrôles intégrés dans les opérations, un deuxième sur la validation des contrôles de premier niveau (le contrôle permanent), et enfin un troisième concernant les contrôles indépendants effectués dans le cadre de missions d'audit périodiques (les contrôles ponctuels).

- **Les stress tests :**

Le stress testing est l'un des outils les plus importants de la prise de décision. Il s'agit de mesurer comment l'entreprise, son bilan, son compte de résultat, son activité résistent à telle situation définie : crise interne, crise économique, crise politique, catastrophe naturelle ou technologique… Ils permettent de mesurer la résilience de l'entreprise à des situations adverses pour les risques de marché, les risques de souscription, les risques de crédit et les risques opérationnels.

- **Le reporting :**

Les entreprises sont généralement confrontées à des exigences de reporting différentes dans chacun des territoires où elles opèrent. Ce reporting permet de rendre compte périodiquement des indicateurs de performance et ils aident très souvent à la prise de décisions. Il existe de nouveaux reporting proposés par Solvabilité II, dont certains deviennent également des outils de reporting internes fondamentaux pour le pilotage de l'entreprise.

- **Les transferts de risque :**

Les transferts de risques permettent de piloter les risques et la solvabilité, au-delà des choix de développement stratégiques. C'est-à-dire qu'une entreprise qui a pour objectif de faire évoluer son profil de risque en diminuant son exposition utilisera des techniques de transfert de risque, et un traité de réassurance élargi diminuera son exposition aux risques de dommages dans tel ou tel marché.

Il existe encore de multiples outils rénovés pour une meilleure gestion de risques comme la culture de l'entreprise et ses techniques d'animation de groupe, les techniques issues du monde de l'analyse décisionnelle tel que le « Reference Class Forecasting », la matrice des risques, les formulaires et les registres, la formation continue…etc. (F. CORDEL, 2013)

2. Les acteurs de l'ERM

Il est indispensable que les activités et actions des acteurs du processus de management des risques soient coordonnées car ils sont bien nombreux. (IFACI, 2003).

- **Le conseil :** qui veille à l'adéquation, la suffisance et l'efficacité du processus et qui s'assure que ce dernier fasse l'objet d'évaluations régulières ;

- **La direction générale :** qui crée les conditions de mise en œuvre du processus au sein de l'entreprise, et qui est responsable de la conception, de la mise en place et du pilotage son pilotage ;

- **Les comités spécialisés du conseil :** tel que le comité d'audit, le comité des risques… ils examinent les risques et engagements hors bilan significatifs, ils vérifient que les processus et procédures en matière financière sont mis en œuvre et sont efficaces, et ils dirigent et coordonnent la prévention et la

maîtrise des risques liés aux opérations de l'entreprise ;

- **Les auditeurs internes :** qui évaluent et contribuent à l'amélioration du processus de management des risques, et rendent les comptes à la direction générale et au comité d'audit, ils aident également à identifier et évaluer les risques ;

- **Le Risk manager :** chargé d'expliquer le processus aux opérationnels, il aide aussi la direction générale à définir la stratégie du management des risques, en évaluant les risques ;

- **La direction opérationnelle et fonctionnelle :** elle choisit le traitement à appliquer au risque, en collaboration avec le Risk manager, elle détermine le niveau de risque acceptable dans son domaine conformément à la politique de l'entreprise ;

- **Le contrôleur de gestion :** qui a une vision transversale de l'entreprise, aide au déploiement de la cartographie, et contribue à la lisibilité des objectifs à tous les niveaux hiérarchiques et sur tous les processus de l'entreprise, il aide également au suivi des actions engagées pour prévenir ou réduire les risques, en fournissant, notamment, des indicateurs chiffrés ;

- **Les commissaires aux comptes ou les auditeurs externes :** qui peuvent apporter des modèles de cartographie, des méthodologies ou des outils d'analyse des risques, le CAC procède à une identification et une évaluation des risques dans le cadre de sa mission légale de certification des comptes.

3. Phases du processus de management du risque

L'ISO 31000, version 2018 fournit une approche générique, globale et non spécifique du management du risque auquel sont confrontés les organismes, quel que soient leurs types ou contexte. Cette norme peut être utilisé tout au long de la vie de l'organisme et peut être appliqué à toute activité, y compris la prise de décisions à

tous les niveaux.

Ce processus, dans ISO 31000, se décompose en cinq étapes ou activités clés comme le montre la figure ci-dessous.

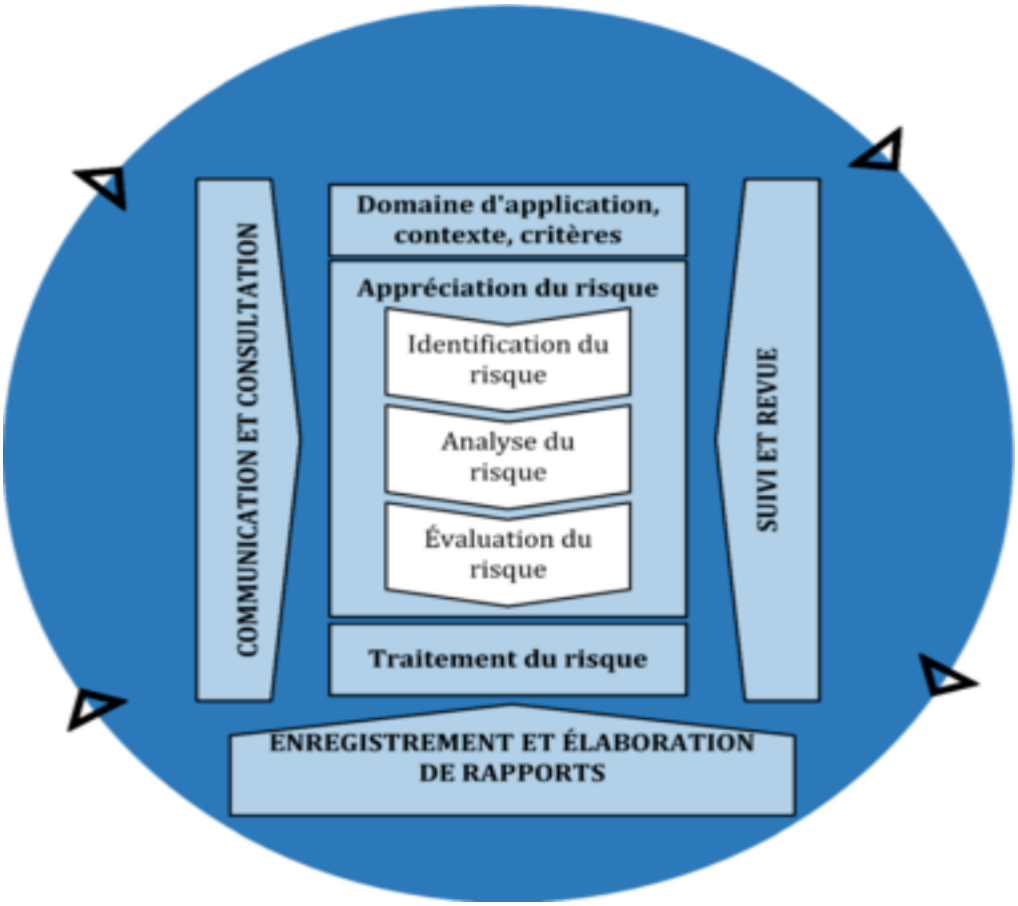


Figure (07) : le processus de management du risque selon la norme ISO31000 à partir de « ISO 31000 :2018(Fr) Management du risque — Lignes directrices ». ISO. https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:fr

3.1. Communication et consultation

Cette première phase qui doit être présente à toutes les étapes du processus, coordonne entre communication et consultation, a pour but de sensibiliser et d'aider

les parties prenantes à comprendre le risque et les principes de prise de décisions. Ceci grâce à des échanges d'informations pertinents, précis et compréhensibles, et d'hypothèses de travail communes avec les parties liées en interne et en externe, ce qui va permettre une même vision du dispositif de management des risques à mettre en œuvre.

La communication et la consultation visent à réunir différents domaines d'expertise et assurent la prise en compte d'une pluralité de point de vue lors de l'évaluation du risque. Et fournir suffisamment d'informations nécessaire à la surveillance du risque et à la prise de décision.

3.2. Etablissement du contexte

Le but de cette phase est de comprendre l'environnement dans lequel l'organisation fonctionne en tenant compte des contraintes et opportunités externes (social, culturel, réglementaire, politiques et économique). Mais aussi des facteurs internes (la stratégie, les objectifs à attendre, les ressources et outils techniques mises en œuvre pour anticiper et apprécier les risques).

Ceci afin de mieux adapter le processus de management du risque, en permettant une appréciation et un traitement du risque efficace et approprié. En d'autres mots, définir le contexte dans lequel évolue l'organisation.

Une partie de cette phase consiste à élaborer les critères du risque qui vont permettre de connaitre le type du risque et d'évaluer son importance. Les critères doivent refléter la perception des parties prenantes, et les exigences légales ou réglementaires concernant les valeurs, les ressources et politiques en place en matière de management du risque.

Pour établir les critères de risques, ces éléments sont à prendre en considération :

- La nature et le type d'incertitudes pouvant avoir une incidence sur les résultats et les objectifs ;
- La façon dont sont définies et mesurées les conséquences et les vraisemblances de ces risques ;
- Les facteurs liés au temps ;
- La cohérence dans l'utilisation des mesures ;
- La méthode de détermination du niveau de risque ;
- La façon dont les combinaisons et séquences de plusieurs risques sont prises en compte ;
- La capacité de l'entreprise.

L'établissement du périmètre d'application, du contexte et des critères a pour but

d'adapter le processus de management du risque, en permettant une appréciation du risque efficace et un traitement du risque approprié.

Le périmètre d'application, le contexte et les critères impliquent de définir le périmètre d'application du processus et de comprendre le contexte interne et externe.

3.3. Appréciation du risque

L'appréciation du risque se définit comme le processus global d'identification, d'analyse et d'évaluation du risque. Elle doit être menée de façon systématique, itérative et collaborative, en s'appuyant sur les connaissances et les opinions des parties prenantes. Il convient d'utiliser les meilleures informations disponibles, complétées si nécessaire par une enquête plus approfondie.

3.3.1. Identification du risque

Consiste à réaliser une cartographie des risques qui peuvent aider ou empêcher l'entreprise à atteindre ses objectifs. La norme ISO 31000 s'intéresse particulièrement aux risques liés à la non-saisie d'une opportunité, car elle couvre à la fois les dimensions Corporate
et business Risk management.

Il existe de nombreux facteurs à prendre en compte, ainsi que leurs relations, pour identifier les incertitudes pouvant avoir une incidence sur un ou plusieurs objectifs. On peut citer par exemple les sources de risque tangibles et intangibles, les causes et événements, menaces et opportunités, vulnérabilités et capacités, indicateurs de risques émergents, conséquences et leur impact sur les objectifs, facteurs liés au temps…

L'organisme, pour son intérêt, doit identifier les risques, que leurs sources soient ou non sous son contrôle. Et de tenir compte du fait qu'il peut y avoir plusieurs types de résultat pouvant avoir diverses conséquences tangibles ou intangibles.

3.3.2. Analyse du risque

L'objectif de cette analyse est de saisir la nature et les caractéristiques du risque en prenant compte de plusieurs facteurs tel que la source du risque, la vraisemblance d'événements, la nature et l'importance de leurs conséquences et l'efficacité des moyens de maîtrise…

L'analyse du risque permet de prendre une décision quant au traitement du risque ou non, et aide à établir la stratégie et les méthodes les plus performantes. Cette étape peut être simple ou complexe selon la disponibilité et la fiabilité des informations et ressources, les divergences d'opinions sur le risque, et les jugements qu'il faut prendre en compte, documentées et communiquées aux décideurs.

Les techniques d'analyse peuvent être qualitatives, quantitatives, ou une combinaison de celles-ci, selon la gravité des conséquences d'événements incertains et difficiles à quantifier.

Pour réaliser une bonne analyse du risque, on doit prendre en considération certaines informations tel que :

- La vraisemblance des événements et des conséquences ;
- La nature et l'importance des conséquences ;
- La complexité et l'interconnexion ;
- Les facteurs liés au temps et la volatilité ;
- L'efficacité des moyens de maîtrise existants ;
- Les niveaux de sensibilité et de confiance.

3.3.3. Évaluation du risque

Consistant à comparer les résultats de l'analyse du risque aux critères de risque établis, l'évaluation du risque aide dans la prise de décision par rapport aux actions supplémentaires à entreprendre ou pas concernant le risque en prenant compte le contexte et les conséquences réelles et perçues par les parties prenantes externes et internes. Les décisions peuvent être : ne rien faire, maintenir les moyens existants, examiner les options de traitement, entreprendre une analyse plus approfondie afin de mieux comprendre le risque et réexaminer les objectifs).

Le résultat de l'évaluation du risque doit être enregistré, communiqué, puis validé aux niveaux appropriés de l'organisme.

3.4. Traitement du risque

L'objectif de cette étape est de choisir les options et les actions à entreprendre qui vont permettre la suppression du risque ou de le réduire à un niveau acceptable. Mais aussi d'apprécier l'efficacité des actions déjà menées pour le traitement du risque, et envisager un traitement complémentaire dans le cas où l'existence du risque résiduel n'est pas acceptable.

Diverses options peuvent être envisager pour traiter le risque nous pouvons citer :

- La décision d'arrêter une activée porteuse du risque ou de commencer une nouvelle ;

- Maintenir ou dupliquer l'apparition du risque via des investissements d'opportunités ;
- Supprimer la source du risque grâce des outils de protection ;
- Partager ou transférer le risque entre parties prenantes via des contrats d'assurances ;
- La décision de modifier la vraisemblance et les conséquences du risque.

Afin de bien choisir l'action à entreprendre, l'organisme se doit de prendre en compte ses obligation, comparer les avantages d'atteinte des objectifs par rapport aux coûts, et tenir compte des valeurs et de l'implication des parties prenantes car certains traitements du risque peuvent être plus acceptables chez certains et non chez les autres, sans oublier les critères du risque et des ressources disponibles.

Le traitement du risque peut engendrer d'autres risques ou conséquences inattendues qui doivent être gérer. C'est pour cela que le suivi et la revue doivent faire partie intégrante de la mise en œuvre du traitement du risque. Et si aucune option ne permet de traiter le risque, ce dernier doit être enregistrer et mis sous contrôle de façon permanente.

Une fois les options de traitements choisis, un plant intégré au processus de management de l'organisation est mis en place pour préciser la manière et l'ordre dont elles vont être appliquer afin de permettre une compréhension et un suivi par les personnes concernées.

Les informations fournies dans le plan de traitement doivent comporter :

- La justification du choix et des avantages attendues des options de traitement proposées ;
- Le moment où les actions sont censées être entreprises et achevées ;
- Les personnes responsables de l'approbation et de la mise en œuvre du plan ;
- Les ressources nécessaires, en tenant compte des impondérables ;
- Les mesures des performances et les contraintes ;
- Les rapports et le suivi requis.

3.5. Surveillance et revue

L'objectif de cette phase est de veiller à l'efficacité du processus de management des risques en améliorant la qualité de sa conception, sa mise en œuvre et les résultats obtenues. Cette phase passe par la construction d'un système d'information management des risques permettant de planifier un suivie périodique du risque et de définir les responsabilités.

La surveillance et la revue ont lieu à toutes les étapes du processus car ils veillent à l'efficacité des contrôles et à détecter tout risques émergents ou changements de contextes en externe ou en interne.

Cette phase se compose de cinq étapes semblables à celle de l'ARM : (Pascal Kerebel, 2009)

- Identification et analyse des risques (étude de la sinistralité antérieure, simulation de l'impact d'un sinistre majeur sur les objectifs stratégiques, quantification des pertes générées par un sinistre majeur) ;
- Étude des outils de contrôle des risques (contrôle interne, technique et financier des risques) ;
- Choix optimal en termes de combinaison d'outils (basé sur les critères de la minimisation des impacts) ;
- Mise en œuvre des décisions (dont budgétisation) ;
- Reporting, monitoring (tableaux de bord management des risques).

Le processus de management du risque et ses résultats sont documentés et font l'objet de rapports, dans le but de les communiquer au sein de l'organisme, fournir des informations pour la prise de décision, améliorer le management du risque, faciliter l'échange d'informations et l'interaction avec toutes les parties prenantes.

L'élaboration de rapports fait partie intégrante de la gouvernance de l'organisme et il convient de prendre en considération :

- Le coût et la méthode de rédaction du rapport ;
- Les besoins et exigences des différentes parties prenantes ;
- La pertinence des informations par rapport aux objectifs de l'organisme et à la prise de décisions.

Une fois que les résultats du processus de management des risques sont apparus, Il est essentiel d'adopter une stratégie relative aux résultats du processus de management des risques :

- Accepter en ne lançant aucune action tout en continuant à superviser, lorsque plus rien d'autre ne fonctionne, il s'agit donc d'assumer la responsabilité et d'accepter les conséquences ;

- Eviter complètement les risques malgré que ce soit presque impossible d'éviter les menaces, ou l'exploiter si c'est une opportunité ;

- Atténuer les risques en prenant des mesures afin de maitriser ceux qui sont inévitables et de réduire les dommages qu'ils peuvent causer. Ou accroître, lorsqu'il s'agit d'une opportunité, la probabilité d'occurrence et la sévérité des impacts ;

- Transférer les risques à d'autres parties, pour qu'elle supporte ses conséquences et sa responsabilité, ou partager avec elles les bénéfices s'il s'agit d'une opportunité.

Section 2 : la gestion des risques et le contrôle interne

Chaque entreprise veille à l'existence des dispositifs de gestion des risques et de contrôle interne de façon à ce qu'ils soient adaptés à ses caractéristiques propres, et qu'ils participent de manière complémentaire à la maîtrise de ses activités. Le dispositif de gestion des risques vise à identifier et analyser les principaux risques de l'entreprise, en utilisant des contrôles qui relèvent du dispositif de contrôle interne. Dans cette section nous allons traiter le contrôle interne, ainsi que sa relation avec l'ERM.

1. Principes généraux du CI

Le cadre de référence de l'AMF (2010) défini le contrôle interne comme un dispositif d'une organisation, défini et mis en œuvre sous sa responsabilité, qui

comprend un ensemble de moyens, de comportements, de procédures et d'actions adaptés aux caractéristiques propres de chaque entreprise qui contribue à la maîtrise de ses activités, à l'efficacité de ses opérations et à l'utilisation efficiente de ses ressources. Et qui doit lui permettre de prendre en compte de manière appropriée les risques significatifs, qu'ils soient opérationnels, financiers ou de conformité.

Le dispositif vise plus particulièrement à assurer la conformité aux lois et règlements, ainsi que l'application des instructions et des orientations fixées par la direction générale, le bon fonctionnement des processus internes de l'entreprise, notamment ceux concourant à la sauvegarde de ses actifs, et enfin la fiabilité des informations financières.

Le contrôle interne ne se limite pas à un ensemble de procédures ou aux seuls processus comptables et financiers. La définition du contrôle interne ne recouvre pas toutes les initiatives prises par les organes dirigeants ou le management comme par exemple la définition de la stratégie de la société, la détermination des objectifs, le traitement des risques ou le suivi des performances.

1.1. Composantes

Le cadre de référence de l'AMF (2010) propose cinq composantes du dispositif de contrôle interne, qui sont les suivantes :

- **Une organisation :** qui définit clairement les responsabilités, qui dispose des ressources et des compétences adéquates, et qui s'appuie sur des systèmes d'informations, sur des procédures ou modes opératoires, et sur des outils et des pratiques appropriés.

  Le contrôle interne est mis en œuvre en se reposant sur des principes fondamentaux et sur une organisation appropriée qui fournit le cadre dans lequel les activités visant à la réalisation des objectifs sont planifiées, exécutées, suivies et contrôlées. Le dispositif repose aussi sur des responsabilités clairement définies, qui peuvent être formalisées et communiquées au moyen de descriptions de tâches, d'organigrammes hiérarchiques et fonctionnels, de délégations de pouvoirs, elles devraient ainsi respecter le principe de séparation des tâches.

  Une politique de gestion des ressources humaines est nécessaire pour la mise en place du dispositif, car elle permet à l'entreprise de disposer des personnes possédant les connaissances et compétences nécessaires à l'exercice de leurs responsabilités et à l'atteinte des objectifs.

Les systèmes d'informations adaptés aux objectifs actuels de l'organisation et conçus de façon à pouvoir supporter ses objectifs futurs, sont aussi primordial à la mise en place du dispositif de contrôle interne.

Le dispositif s'appuie sur des procédures ou modes opératoires qui précisent la manière dont devrait s'accomplir une action ou un processus, sur des outils ou instruments de travail (bureautique, informatique) qui doivent être adaptés aux besoins de chacun et auxquels chaque utilisateur devrait être dûment formé, et enfin des pratiques communément admises au sein de la société.

- **Une diffusion en interne d'informations** : les informations diffusées doivent être pertinentes et fiables, dont la connaissance permet à chacun d'exercer ses responsabilités.

  La société devrait disposer de processus qui assurent la communication de ces informations, et leur diffusion en temps opportun aux acteurs concernés de l'entreprise afin de leur permettre d'exercer leurs responsabilités.

- **Un dispositif de gestion des risques** : visant à recenser, analyser et traiter les principaux risques identifiés au regard des objectifs de la société.

- **Des activités de contrôle** : qui doivent être proportionnées aux enjeux propres à chaque processus, et conçues pour s'assurer que les mesures nécessaires sont prises en vue de maîtriser les risques susceptibles d'affecter la réalisation des objectifs. Les activités de contrôle sont présentes partout dans l'organisation, à tout niveau et dans toute fonction qu'il s'agisse de contrôles orientés vers la prévention ou la détection, de contrôles manuels ou informatiques ou encore de contrôles hiérarchiques.

- **Une surveillance permanente** : comme tout système, le dispositif de contrôle interne doit faire l'objet d'une surveillance permanente accompagnée d'un examen régulier de son fonctionnement, il s'agit de vérifier sa pertinence et son adéquation aux objectifs de l'entreprise.

1.2. Objectifs

Selon le cadre de référence de l'AMF (2010), les objectifs du dispositif de contrôle interne visent, plus particulièrement à assurer :

- **La conformité aux lois et règlements :**

Il s'agit des lois et règlements auxquels l'entreprise est soumise, et qui fixent des normes de comportement qu'elle intègre à ses objectifs de conformité. Il est nécessaire que l'entreprise dispose d'une organisation lui permettant de connaître les diverses règles qui lui sont applicables, d'être informée en temps utile des modifications qui leur sont apportées, de transcrire ces règles dans ses procédures internes, et d'informer et former les collaborateurs sur celles des règles qui les concernent.

- **L'application des instructions et des orientations :**

Il s'agit de celles de la direction générale qui permettent aux collaborateurs de comprendre ce qui est attendu d'eux et de connaître l'étendue de leur liberté d'action. Ces instructions et orientations doivent être communiquées aux collaborateurs concernés, en fonction des objectifs assignés à chacun d'entre eux, afin de fournir des orientations sur la façon dont les activités devraient être menées, elles doivent être aussi établies en fonction des objectifs poursuivis par la société et des risques encourus.

- **Le bon fonctionnement des processus internes :**

Notamment ceux visant à la sauvegarde des actifs, tel que les processus opérationnels, industriels, commerciaux et financiers. Le bon fonctionnement des processus exige l'établissement des normes de fonctionnement et la mise en place des indicateurs de suivi.

- **La fiabilité des informations financières :**

Qui ne peut s'obtenir que grâce à la mise en place de procédures de contrôle interne visant à la bonne prise en compte des opérations réalisées par l'entreprise. La qualité du dispositif de contrôle interne peut-être recherchée au moyen d'une séparation des tâches qui permet de bien distinguer les tâches d'enregistrement, les tâches opérationnelles et les tâches de conservation. Au moyen aussi d'une description des fonctions qui permet l'identification des origines des informations produites, et leurs destinataires.

Enfin au moyen d'un système de contrôle interne comptable qui s'assure que les opérations sont effectuées conformément aux instructions générales et spécifiques, et qu'elles sont comptabilisées de manière à produire une information financière conforme aux principes comptables généralement admis.

2. Articulation entre CI et ERM

Pour l'autorité Des Marchés Financiers (AMF, 2010), le contrôle interne et le processus de management des risques sont complémentaires. Étant donné que ce dernier s'appuie sur le CI pour intégrer des contrôles sécurisant son bon fonctionnement, dans le but d'identifier et d'analyser les principaux risques de la société. De son côté le CI s'appuie sur le processus de management des risques pour identifier et maîtriser ces risques.

L'articulation entre ces deux dispositifs sont conditionnés par la culture du risque et du contrôle propres à la société, le style de management, les valeurs éthiques de la société.

Dans son étude, Sourour (2018) a parlé de la relation entre le contrôle interne et le processus de management des risques en évoquant deux notions, la complémentarité et la substitution.

2.1. La complémentarité entre CI et ERM

L'ERM est le prolongement ou une extension du contrôle interne qui est considérer comme un mécanisme de gouvernance de l'entreprise, dans le but de réduire les risques auxquels elle s'expose. Le schéma suivant, nous montre que l'ERM complète les composantes du CI en ajoutant trois paramètres tel que le traitement des risques, et un quatrième objectif qui est la stratégie.

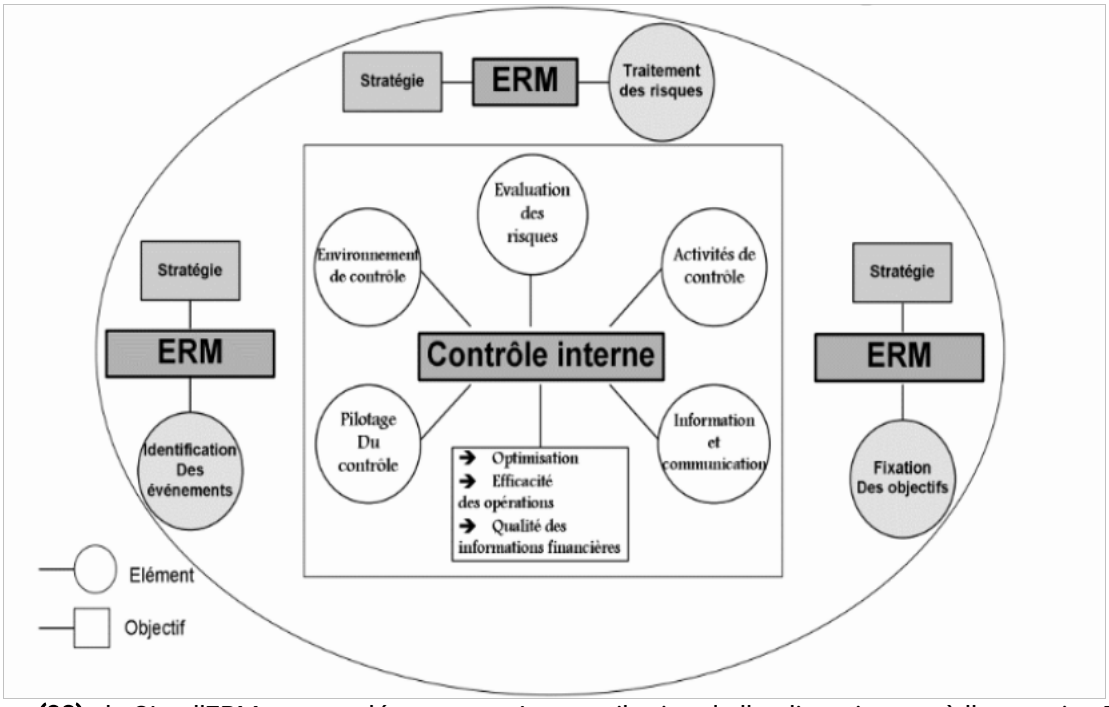


Figure (08) : le CI et l'ERM se complémentent, « La contribution de l'auditeur interne à l'entreprise Risk Management : résultats d'une étude exploratoire ». Sourour. 2018, p05.
https://www.researchgate.net/publication/331251058

COSO après avoir bien élaborer le cadre de l'ERM. Il a bien précisé que la fonction d'audit interne se doit d'aider la direction dans l'évaluation de l'efficacité du risque d'entreprise à travers le contrôle interne.

2.2. La substitution entre ERM et CI

A la fin de son étude, Sourour (2018) a écarté l'hypothèse selon laquelle l'ERM est un prolongement du contrôle Interne par rapport à sa contribution dans la fonction d'audit interne. Il a plutôt adopté l'hypothèse de la substitution.

Malgré que le contrôle interne soit la base de la fiabilité et de la transparence de l'information, il n'empêche qu'il a plusieurs failles. Une entreprise qui ne possède pas une fonction d'audit interne aura du mal à avoir un reporting sur le CI réussit. Car pour piloter et syntoniser les informations de ce dernier elle aura besoin de l'AI qui est en lien direct avec la direction générale. Une étude de l'efficacité du contrôle interne, à la charge de l'AI, montre la pauvreté du contenu informationnel de son reporting et la remise en cause de l'argumentation selon laquelle le contrôle interne pourrait améliorer la fiabilité de l'information. La volonté de dépasser ces failles à pousser vers le souhait de remplacer le contrôle interne par la gestion des risques.

L'engagement du management vis-à-vis de l'AI, la légitimité de la contribution de l'AI vis-à-vis de l'ERM et la relance du contrôle interne expliquent cet effet de substitution du contrôle interne vers l'ERM, schéma ci-dessous :

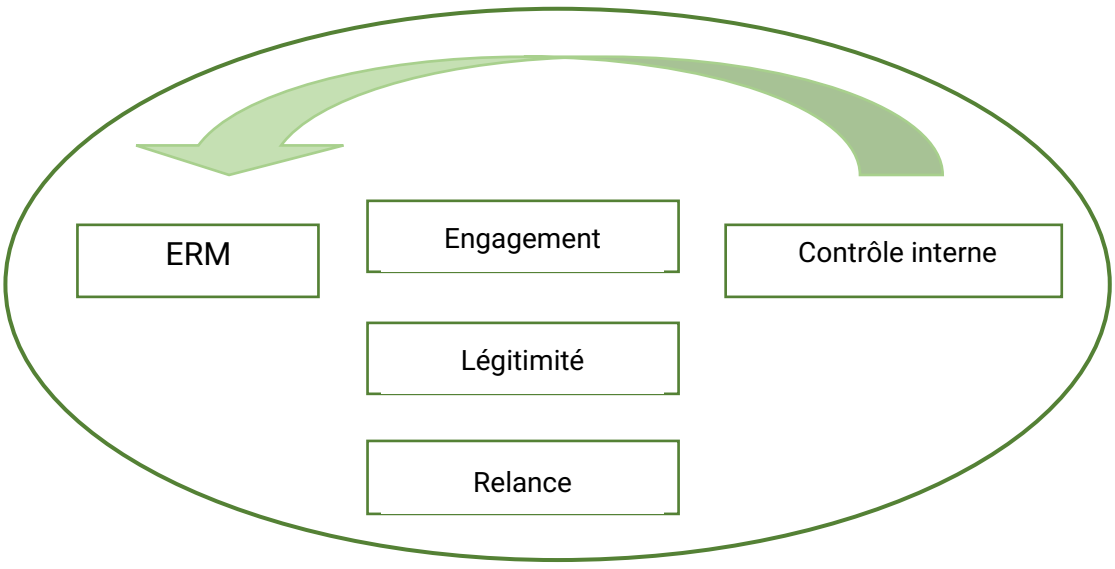


Figure (09) : le contrôle interne et l'ERM se substituent à partir de « La contribution de l'auditeur interne à l'entreprise Risk Management : résultats d'une étude exploratoire ». Sourour. 2018, p05. https://www.researchgate.net/publication/331251058

La Direction Générale a le devoir de concourir à la croissance, la performance et à la pérennité de l'organisation. Pour cela elle est dans l'obligation de concevoir et

de gérer des dispositifs efficaces de gestion des risques et de contrôle interne, et s'assurer qu'ils pourront répondre aux objectifs pour lesquels ils ont été conçues, qui est la maîtrise des risques.

Et plus particulièrement, la DG doit veiller à ce que le CI et l'ERM fonctionnent de manière coordonnée pour réaliser les activités suivantes : (Institut Français Des Administrateurs, 2013)

- Cartographie et évaluation des risques
- Définition et évaluation des activités de contrôle
- Plans de remédiation
- Pilotage et diffusion de l'information
- Supervision continue

Le modèle des « trois lignes de défense » fournit des recommandations utiles sur la définition claire des responsabilités en matière de gestion des risques et de contrôle interne.

3. Les trois lignes de défense « 3 LoD »

Le modèle des trois lignes de défense « 3 LoD » identifié par l'IIA est de plus en plus utilisé comme référence pour évaluer l'efficacité, contrôler la communication et séparer les rôles et responsabilités des acteurs de la gouvernance d'entreprise. La Direction Générale est au cœur du dispositif de maîtrise globale des risques. Sa structure en trois lignes de défense est une approche pertinente des rôles et responsabilités du management opérationnel, des fonctions transverses, et de l'audit interne. (Weekes-Marshall, 2020)

Plus particulièrement, 3 LoD est utilisé pour évaluer l'efficacité de la gestion des risques, car il fournit une manière simple et efficace de s'assurer que l'ERM et le contrôle interne sont coordonnées et complémentaires au sein d'une organisation. (WIPO, 2016)

3.1. La première ligne de défense :

Constituée par la direction opérationnelle de l'organisation dont la responsabilité est d'identifier, d'évaluer, de contrôler et d'atténuer les risques, en mettant en œuvre un dispositif de contrôle adéquat, portant sur les processus dont elle a la charge. Est une fonction qui possède et gère le risque en même temps, permet de maîtriser les activités au jour le jour en mettant en œuvre des pratiques

efficaces de gestion des risques au niveau de chaque processus et en communiquant les informations appropriées à la deuxième ligne de maîtrise. (IFA, 2013)

Cette première ligne a pour rôle, selon le modèle des trois lignes de l'IIA (2020) :

- D'orienter et de conduire les actions, notamment le management des risques, et exploiter les ressources à disposition pour réaliser les objectifs de l'organisation.

- Entretenir un dialogue permanent avec l'organe de gouvernance et lui fournir des comptes-rendus sur les résultats prévisionnels et réalisés au regard des objectifs de l'organisation, et des risques.

- De mettre en place et de préserver les structures et les processus adéquats pour le management des opérations et des risques, y compris le contrôle interne.

- De veiller au respect des exigences d'ordre juridique, réglementaire et éthique.

3.2. La deuxième ligne de défense

En plus des services fonctionnels responsables de domaines d'expertise, cette deuxième ligne contient les fonctions de gestion des risques, de contrôle interne, d'assurance, de conformité… qui rentrent dans l'animation du dispositif global de maîtrise des risques, notamment en : (IFA, 2013)

- Assistant les opérationnels dans l'identification et l'évaluation des principaux risques relevant de leur domaine d'expertise, et à concevoir des contrôles pertinents ;

- Proposant des politiques et des procédures de groupe par domaine d'activité ;

- Développant les meilleurs pratiques et les échanges ;

- Observant et en rendant compte du fonctionnement effectif des processus.

Ces services possèdent une expertise et un savoir-faire uniques pour l'analyse des organisations et des compétences essentielles en matière d'activités de contrôle, ce qui aident les propriétaires des risques à communiquer les informations adéquates sur ces risques à l'ensemble de l'organisation.

Le modèle des trois lignes de l'IIA (2020), précise les rôles suivants pour cette ligne :

- Apporter une expertise complémentaire, une assistance, un suivi et des critiques constructives en matière de gestion des risques concernant le développement, la mise en œuvre et l'amélioration continue des pratiques de gestion des risques et la relation entre ces pratiques, y compris le contrôle interne

- Produit des analyses et des rapports sur l'adéquation et l'efficacité de la gestion des risques (contrôle interne y compris)

Ces premières lignes peuvent être fusionner, car tous les deux contribuent à l'atteinte des objectifs de l'organisation. La première couvre les fonctions supports et fournis les produits et services demandés par les clients de l'organisation. Quant à la deuxième ligne, elle recouvre les activités d'appui à la gestion des risques. Ceci fait partie de l'un des principes du model des trois lignes de défense de l'IIA qui explique que :

Certains rôles de deuxième ligne peuvent être confiés à des spécialistes chargés d'apporter une expertise complémentaire, une assistance, un suivi et des critiques constructives aux acteurs de la première ligne. D'autres peuvent être orientés sur des objectifs précis dans le domaine de la gestion des risques (conformité aux lois et règlements et comportement éthique acceptable, contrôle interne, sécurité des systèmes d'information, développement durable, assurance qualité…), et même se voir confier de plus grandes responsabilités en la matière, comme le management des risques de l'entreprise (ERM). Pour autant, la gestion des risques demeure l'apanage des rôles de première ligne et s'inscrit dans le périmètre d'action du management. (2020, p. 3)

3.3. La troisième ligne de défense :

A travers une approche fondée sur le risque, cette dernière ligne a pour mission de fournir une assurance globale objective et indépendante du management, sur l'adéquation et l'efficacité des deux premières lignes de maîtrise et de la gouvernance de la gestion des risques, aux instances de surveillance et à la direction générale de l'organisation.

N'étant autre que la fonction d'audit interne, elle doit être directement rattaché au plus haut niveau de l'organe de gouvernance, jouir d'un accès total aux ressources humaines, matérielles et informationnelles nécessaires à l'exercice de ses fonctions, et planifier et fournir ses services en toute indépendance et objectivité. (IFA, 2013)

Le rôle de l'audit interne ici est bien précisé par IIA (2020) :

- Rend compte en premier lieu à l'organe de gouvernance et préserve son indépendance vis-à vis du management ;

- Fournit une assurance et des conseils indépendants et objectifs au management et à l'organe de gouvernance sur l'adéquation et l'efficacité de la gouvernance et de la gestion des risques (contrôle interne y compris) afin de contribuer à la réalisation des objectifs de l'organisation et de promouvoir et favoriser l'amélioration continue ;

- Alerte l'organe de gouvernance des atteintes éventuelles à son indépendance et à son objectivé et prend les mesures de protection qui s'imposent.

De manière général, cette fonction fournit une assurance indépendante par le biais d'une approche fondée sur les risques, à l'organe directeur et à la direction générale de l'organisation quant à l'efficacité avec laquelle l'organisation évalue et gère ses risques, y compris la manière dont les première et deuxième ligne de défense fonctionnent.

Le schéma qui va suivre illustre ces trois lignes de défense et la relation qu'elles ont avec la direction générale et le conseil d'administration :

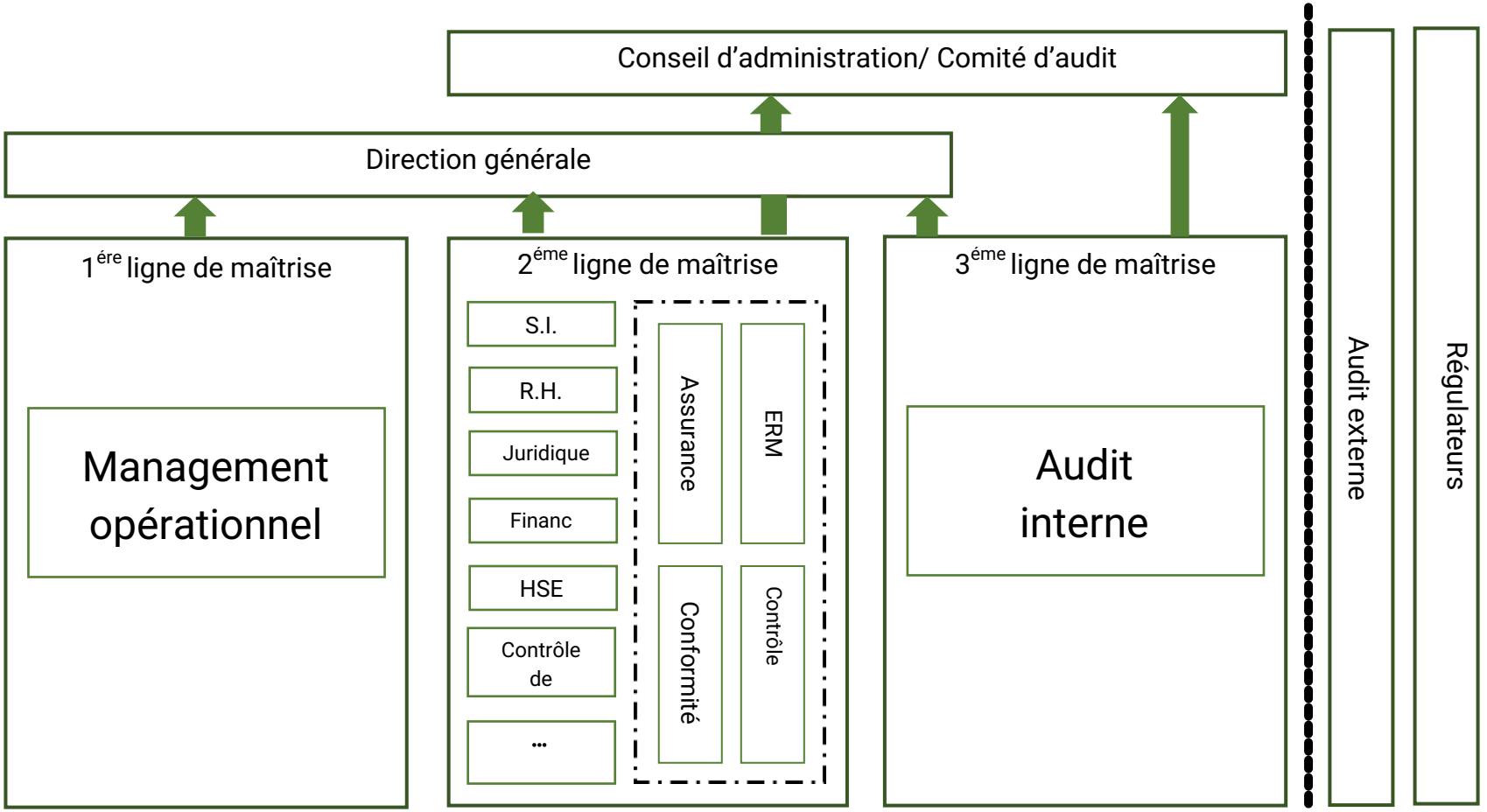


Figure (10) : les trois lignes de défense à partir de « Trois lignes de Maîtrise pour une meilleure performance », IFA, 2013, p.06, AMRAE – IFACI https://docs.ifaci.com/wp-content/uploads/2018/03/Trois_lignes_de_ma%C3%AEtrise_pour_une_meilleure_performance.pdf

Section 3 : la contribution de l'audit interne dans l'amélioration du processus ERM

Dans cette section, nous allons aborder les concepts fondamentaux liés à l'audit interne ainsi qu'à sa mission, nous allons aussi traiter son rôle quant au management des risques, et sa contribution à l'amélioration de l'efficacité du processus ERM selon trois approches.

1. Déroulement d'une mission d'audit interne :

1.1. Cadre de référence d'un audit ERM

L'IFACI (2017) propose la norme IIA 2120 : Management des risques **«** L'audit interne doit évaluer l'efficacité des processus de management des risques et contribuer à leur amélioration *»*

Par le biais du jugement professionnel des auditeurs internes, on arrive à déterminer si les processus de management des risques sont efficaces, et pour cela, ils vérifient :

- La cohérence des objectifs de l'organisation avec sa mission et leur contribution ;
- L'identification et l'évaluation des risques significatifs ;
- Les modalités de traitement des risques retenues, si elles sont appropriées et en adéquation avec l'appétence pour le risque de l'organisation ;
- La communication en temps opportun au sein de l'organisation des informations relatives aux risques, pour permettre aux collaborateurs, à leur hiérarchie et au Conseil d'exercer leurs responsabilités.

L'audit interne peut s'appuyer sur des informations issues de différentes missions afin d'étayer cette évaluation. Une vision consolidée des résultats de ces missions permet une compréhension du processus de management des risques de l'organisation et de son efficacité.

La surveillance du processus de management des risques est effectuée au moyen d'activités courantes de management, d'évaluations distinctes ou par ces deux moyens.

La série IIA 2120 rassemble 5 normes :

- **2120.A1** : L'audit interne doit évaluer les risques afférents à la gouvernance, aux opérations et aux systèmes d'information de l'organisation au regard de l'atteinte des objectifs stratégiques de l'organisation, de la fiabilité et l'intégrité des informations financières et opérationnelles, de l'efficacité et l'efficience des opérations et des programmes, de la protection des actifs, et du respect des lois, règlements, règles, procédures et contrats.

- **2120.A2** : L'audit interne doit évaluer la possibilité de fraude et la manière dont ce risque est géré par l'organisation.
- **2120.C1** : Au cours des missions de conseil, les auditeurs internes doivent couvrir les risques liés aux objectifs de la mission et demeurer vigilants vis-à-vis de l'existence de tout autre risque susceptible d'être significatif.

- **2120.C2** : Les auditeurs internes doivent utiliser leurs connaissances des risques acquises lors de missions de conseil, pour évaluer les processus de management des risques de l'organisation.

- **2120.C3** : Lorsque les auditeurs internes accompagnent le management dans la conception et l'amélioration des processus de management des risques, ils doivent s'abstenir d'assumer une responsabilité opérationnelle en la matière.

1.2. Concepts de base

L'IFACI (2002) définit l'audit interne comme une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, qui lui apporte ses conseils pour les améliorer, et qui contribue à créer de la valeur ajoutée.

Il contribue à l'atteinte d'objectifs d'une entreprise en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle, et de gouvernement d'entreprise, et en faisant des propositions pour renforcer leur efficacité.

1.2.1. Principes de l'audit interne

Il existe un référentiel professionnel que l'IFACI a établi (en 2012) afin de présenter les exigences que la direction d'audit interne doit respecter, et qui sont sous trois formes, à savoir :

- **Des exigences de moyens** :

- L'indépendance du service d'audit interne.
- Une charte d'audit interne doit être établi au préalable afin de définir de manière formelle les missions, les pouvoirs et les responsabilités de ce service.
- Le code de déontologie doit être respecté par les auditeurs internes.
- Les auditeurs internes doivent effectuer leurs travaux avec objectivité.
- Les auditeurs internes doivent être compétents et ils doivent apporter à leur travail la diligence et le savoir-faire.
- Le responsable de l'audit interne doit veiller à ce que les ressources affectées à l'activité d'audit interne soient adéquates, suffisantes et mises en œuvre de manière efficace pour réaliser le plan d'audit approuvé.
- Le service d'audit interne doit posséder ou acquérir les connaissances, le savoir-faire et les autres compétences nécessaires à l'exercice de ses responsabilités collectives et individuelles.
- Les auditeurs internes doivent améliorer leurs connaissances, savoir-faire et autres compétences par une formation professionnelle continue.
- Le responsable de l'audit interne doit établir des règles et procédures fournissant un cadre à l'activité d'audit interne.

- **Des exigences de prestation :**

- L'audit interne doit évaluer le processus de gouvernement d'entreprise et formuler les recommandations appropriées en vue de son amélioration, sur la base d'une approche systématique et méthodique.
- L'audit interne doit évaluer l'efficacité et contribuer à l'amélioration des processus de management des risques et du dispositif de contrôle interne.
- Le responsable de l'audit interne doit établir un plan annuel ou pluriannuel d'audit

fondé sur les risques, afin de définir les priorités de ce plan cohérentes avec les objectifs de l'organisation.

- Le responsable de l'audit interne doit communiquer à la Direction Générale et au Comité d'audit (ou au Conseil) son plan et ses besoins, pour examen et approbation.
- Les auditeurs internes doivent déterminer le champ et les ressources appropriées et suffisantes pour répondre aux objectifs de la mission.
- Les auditeurs internes doivent informer le management opérationnel audité sur le déroulement de la mission
- A partir des objectifs de la mission, les auditeurs internes doivent concevoir et documenter un plan de mission sur la base d'un examen préliminaire.
- Afin de pouvoir évaluer le dispositif de contrôle, les auditeurs internes doivent déterminer, en liaison avec le management audité, les critères de contrôle interne adéquats pour apprécier si les objectifs des opérations et processus ont été atteints.
- Les auditeurs internes doivent élaborer et documenter un programme de travail permettant d'atteindre les objectifs de la mission.
- Les auditeurs internes doivent identifier, analyser, évaluer et documenter les informations nécessaires pour atteindre les objectifs de la mission.
- Les auditeurs internes échangent sur les principales analyses, conclusions et recommandations de la mission avec les responsables appropriés.
- Les auditeurs internes doivent communiquer les résultats de la mission, en respectant des conditions de fond et de forme.
- Le responsable de l'audit interne doit diffuser les résultats de la mission aux destinataires appropriés.
- Le responsable de l'audit interne doit mettre en place et maintenir un processus de suivi des actions correctives.
- Le responsable de l'audit interne partage les informations et coordonne les activités des prestataires internes et externes de services d'assurance et de conseil.
- Le responsable de l'audit interne doit rendre compte périodiquement à la Direction Générale et au Comité d'audit (ou au Conseil) des résultats obtenus.

- **Des exigences de pilotage :**

- Le service d'audit interne doit faire l'objet d'un pilotage approprié afin d'apporter de la valeur à l'organisation.
- Les missions d'audit interne doivent faire l'objet d'une supervision appropriée.
- Le responsable de l'audit interne doit élaborer et tenir à jour un programme d'assurance et d'amélioration qualité portant sur tous les aspects de l'audit interne et permettant un contrôle continu de son efficacité.
- Lorsqu'une mission donnée n'a pas été conduite conformément aux normes, la communication des résultats doit l'indiquer.

1.2.2. Normes d'audit interne :

Les normes d'audit interne sont élaborées par l'IIA « Institut of Internal Auditors », l'IFACI (2012) les proposes d'une manière étudiée et commentée. Elles se composent de trois catégories, des normes de qualification, de fonctionnement et de mise en œuvre

Les normes ont pour objet :

- De définir les principes de base que la pratique de l'audit interne doit suivre ;
- De fournir un cadre de référence pour la réalisation et la promotion d'un large éventail
  d'activités d'audit interne apportant une valeur ajoutée ;
- D'établir les critères d'appréciation du fonctionnement de l'audit interne ;
- De favoriser l'amélioration des processus organisationnels et des opérations.

Les normes de qualification : elles énoncent les caractéristiques que doivent présenter les organisations et les personnes accomplissant des activités d'audit interne

- **1000 « Mission, pouvoirs et responsabilités »** : la mission, les pouvoirs et les responsabilités de l'audit interne doivent être formellement définis dans une charte, et ils doivent être cohérents avec les normes et dûment approuvés par le conseil.
- **1100 « Indépendance et objectivité »** : l'audit interne doit être indépendant et

les auditeurs internes doivent effectuer leur travail avec objectivité.

- **1200 « Compétence et conscience professionnelle »** : les missions doivent être remplies avec compétence et conscience professionnelle.
- **1300 « Programme d'assurance et d'amélioration qualité »** : Le responsable de l'audit interne doit élaborer et tenir à jour un programme d'assurance et d'amélioration qualité portant sur tous les aspects de l'audit interne et permettant un contrôle continu de son efficacité. Ce programme inclut la réalisation périodique d'évaluations internes et externes de la qualité ainsi qu'un suivi interne continu. Chaque partie du programme doit être conçue dans un double but : aider l'audit interne à apporter une valeur ajoutée aux opérations de l'organisation et à les améliorer, et garantir qu'il est mené en conformité avec les normes et le code de déontologie.

Les normes de fonctionnement : elles décrivent la nature des activités d'audit interne et définissent des critères de qualité permettant d'évaluer les services fournis.

- **2000 « Gestion de l'audit interne »** : le responsable de l'audit interne doit gérer cette activité de façon à garantir qu'elle apporte une valeur ajoutée à l'organisation. Et ce en établant une planification fondée sur les risques afin de définir les priorités cohérentes avec les objectifs de l'organisation, en communicant à la direction générale et au conseil son plan d'audit et ses besoins et ses résultats, en veillant à ce que les ressources affectées à cette activité soient adéquates, suffisantes et mises en œuvre de manière efficace pour réaliser le plan d'audit approuvé, et en établant des règles et procédures fournissant un cadre à l'activité d'audit interne.
- **2100 « Nature du travail »** : l'audit interne doit évaluer les processus de management des risques, de contrôle et de gouvernement d'entreprise et contribuer à leur amélioration sur la base d'une approche systématique et méthodique. Il doit ainsi aider l'organisation en identifiant et en évaluant les risques significatifs et contribuer à l'amélioration des systèmes de management des risques et de contrôle.
- **2200 « Planification de la mission »** : les auditeurs internes doivent concevoir

et formaliser un programme pour chaque mission. Ce programme précise le champ d'intervention, les objectifs, la date et la durée de la mission, ainsi que les ressources allouées.

- **2300 « Accomplissement de la mission »** : les auditeurs internes doivent identifier, analyser, évaluer et documenter les informations nécessaires pour atteindre les objectifs de la mission. Ils doivent fonder leurs conclusions et les résultats de leur mission sur des analyses et évaluations appropriées.
- **2400 « Communication des résultats »** : les auditeurs internes doivent communiquer les résultats de la mission en incluant les objectifs et le champ de la mission, ainsi que
  les conclusions, recommandations et plans d'actions…La communication doit être exacte, objective, claire, concise, constructive, complète et émise en temps utile.
- **2500 « Surveillance des actions de progrès »** : le responsable de l'audit interne doit mettre en place un processus de suivi permettant de surveiller et de garantir que des mesures ont été effectivement mises en œuvre par le management ou que la direction générale a accepté de prendre le risque de ne rien faire.
- **2600 « Acceptation des risques par la direction générale »** : lorsque le responsable de l'audit interne estime que la DG a accepté un niveau de risque résiduel qui pourrait s'avérer inacceptable pour l'organisation, il doit examiner la question avec elle. S'ils ne peuvent arrêter une décision concernant le risque résiduel, ils doivent soumettre la question au Conseil aux fins de résolution.

Les normes de mise en œuvre : tandis que les normes de qualification et celles de fonctionnement s'appliquent aux travaux d'audit interne en général, les normes de mise en œuvre s'appliquent à des types de missions spécifiques. Il peut exister différents ensembles de normes de mise en œuvre, correspondant chacun à un grand type d'activité d'audit interne. Par exemple les normes concernent les activités d'assurance sont indiquées par la lettre « A » après le numéro de la norme (1130.A1).

1.2.3. Phases d'une mission d'audit interne

L'IFACI dans une fiche méthodologique sur la conduite d'une mission d'audit interne, avance les étapes de la mission ainsi : (s. d.)

- **Préciser les objectifs et le périmètre de la mission** : il s'agit de les préciser en fonction de l'événement déclenchant la mission et conformément aux attentes des clients de la mission.

- **Conduire la réunion d'ouverture** : dont l'objectif est de matérialiser le démarrage officiel de la mission et en expliciter le contenu et les modalités.

- **Analyser les processus et leurs objectifs** : afin de comprendre le domaine audité, ses enjeux, les processus mis en œuvre et leurs objectifs.

- **Identifier et évaluer les risques** : en faisant l'inventaire des événements qui pourraient empêcher l'atteinte des objectifs du domaine audité, et en mesurant leur probabilité de survenance et leur impact.

- **Evaluer la conception du dispositif de contrôle** : et identifier les contrôles clefs existants et évaluer la conception du dispositif de contrôle au regard de référentiels externes s'ils s'appliquent.

- **Valider le référentiel d'audit Etape** : valider avec les audités, la référence à partir de laquelle le dispositif de contrôle interne va être évalué au cours de la mission d'audit.

- **Sélectionner les objectifs d'audit** : toujours dans la planification, il s'agit de définir le périmètre des travaux à réaliser sur le terrain.

- **Elaborer le programme de travail** : et définir les procédures d'audit qui permettront d'atteindre les objectifs d'audit.

- **Ajuster le budget et allouer les ressources** : et ce en évaluant les ressources nécessaires à la mise en œuvre du programme de travail et en identifiant les

ressources disponibles afin de les affecter à la mise en œuvre du programme de travail.

- **Valider l'organisation de la mission** : il s'agit d'approuver formellement le programme de travail.

- **Conduire la réunion de lancement de la phase Accomplissement** : encore une fois, matérialiser le démarrage officiel de la phase Accomplissement de la mission.

- **Collecter les informations et constituer les preuves d'audit** : et surtout obtenir des preuves sur la capacité des dispositifs de contrôle à maîtriser les risques ou non.

- **Valider les preuves d'audit** : il s'agit de valider avec les audités, le résultat des tests d'audit.

- **Analyser les causes, et élaborer les recommandations** : par l'identification des raisons pour lesquelles les contrôles ne sont pas mis en œuvre de façon satisfaisante, et l'élaboration des mesures correctives.

- **Conduire la réunion de clôture** : il s'agit de faire valider par les responsables du domaine audité la cohérence et la formulation définitive de l'ensemble des observations d'audit.

- **Finaliser le plan d'actions** : et documenter les modalités de mise en œuvre opérationnelles des mesures correctives.

- **Rédiger le rapport** : et documenter les résultats définitifs et officiels de la mission d'audit pour diffusion aux clients de la mission.

- **Valider le rapport** : il s'agit d'approuver formellement le rapport d'audit.

Pour la documentation utilisée lors d'une mission d'audit, l'IFACI les énumèrent

comme suit

- **La lettre de mission** : à la première étape, celle de la précision des objectifs et le périmètre de la mission.

- **Le programme de travail** : il prend son rôle à partir de la septième étape celle de sélectionner les objectifs d'audit jusqu'à la douzième, collecter les informations et constituer les preuves d'audit.

- **La fiche de test** : lors de la collecte d'informations et la constitution de preuves, et lors de la validation de ces preuves.

- **La fiche d'observation** : utilisée à l'étape d'analyse des causes et d'élaboration des recommandations.

- **Le rapport d'audit** : dans les quatre dernières étapes, conduire la réunion de clôture, finaliser le plan d'actions, rédiger le rapport, et valider le rapport.

- **La fiche de suivi de mission** : ce document est utilisé durant toutes les phases et étapes.

1.2.4. Outils de l'audit interne

Dans la même fiche méthodologique de L'IFACI on trouve ces outils de conduite d'une mission d'audit interne : (s. d.)

- **Entretien** : dont la finalité est de collecter des informations afin de prendre connaissance des activités du domaine audité et éventuellement constituer les preuves d'audit qui permettront d'atteindre les objectifs de la mission d'audit. Les entretiens sont des situations au cours desquelles les audités et les auditeurs internes peuvent échanger. Ces échanges permettent de construire une relation de travail positive tout au long du déroulement de la mission d'audit.

- **Grille d'analyse des tâches** : elle permet de visualiser les attributions des personnes ou des services, c'est-à-dire d'identifier « qui fait quoi », elle fait sortir aussi les éventuelles inadéquations de la répartition des tâches d'un processus

entre les personnes et les services (ainsi que les tâches non faites).

- **Diagramme de flux** : il sert à représenter graphiquement le déroulement d'un processus, c'est un outil d'aide à la prise de connaissance, un outil de vérification, il permet de synthétiser les informations que l'on pourrait trouver dans la description narrative du déroulement d'un même processus. Il peut aussi être utile pour situer et analyser les dispositifs de contrôle interne.

- **Approche Processus** : afin de décrire de façon méthodique les activités du domaine audité pour d'identifier leurs objectifs, leurs risques et les dispositifs de contrôle qui devraient permettre de maîtriser ceux-ci. Ce dernier Permet de concentrer la mission d'audit sur les objectifs clefs du domaine audité, la satisfaction des clients des processus et l'efficacité des processus, il permet ainsi d'avoir une vision transversale des activités d'une organisation et d'impliquer l'ensemble des acteurs concernés par un processus.

- **Test de cheminement** : il permet une compréhension détaillée du déroulement effectif des différentes étapes d'une opération en impliquant les acteurs concernés directement par celle-ci. Son objectif est de suivre les différentes étapes d'une opération de son origine jusqu'à son dénouement afin de confirmer la compréhension d'un flux de traitement et de ses contrôles avant de faire des tests détaillés sur ceux-ci.

- **Hiérarchisation des risques** : dans le but de sélectionner les risques pour lesquels il sera nécessaire d'évaluer la conception du dispositif de contrôle. Cette hiérarchisation permet de définir le périmètre des travaux d'audit.

- **Référentiel d'audit** : il sert à recenser les objectifs de chacun des processus de l'entité auditée et pour chacun d'eux les risques auxquels ils sont exposés et les contrôles qui devraient permettre de réduire ces risques. Les contrôles identifiés constitueront la référence à partir de laquelle sera réalisée l'évaluation du système de contrôle interne de l'entité auditée. Il permet ainsi de se concentrer sur les contrôles clefs en s'intéressant aux contrôles liés directement aux objectifs du processus.

- **Diagramme Cause / Effet** : il procure un cadre d'analyse dans le but d'accompagner et de structurer les réflexions des auditeurs internes en

collaboration avec les opérationnels lors de l'analyse des causes des dysfonctionnements constatés au cours d'une mission d'audit interne sachant que les actions correctives ou les recommandations ont pour objet de faire disparaître ces causes.

- **Questionnaire de Contrôle Interne** : il permet de structurer le questionnement de façon systématique à partir des dispositifs de contrôle inventoriés dans le RCI en visant l'évaluation des dispositifs de contrôle au regard du référentiel de contrôle interne.

- **Brainstorming** : dans le but de stimuler l'imagination, c'est-à-dire la faculté de produire des idées sur un problème posé tant pour trouver des solutions que pour en rechercher les causes, il permet de faire émerger des solutions qui auraient été censurées ou n'auraient pas été proposées.

- **Piste d'audit** : son objectif est de S'assurer qu'il est possible de remonter à l'origine d'une opération, elle permet une compréhension détaillée et circonstanciée des mécanismes assurant la traçabilité des opérations.

- **Circulation** : elle permet d'obtenir des preuves d'une grande fiabilité, en demandant à un tiers externe à l'organisation une vérification de la même information collectée
  au sein de l'organisation.

- **Procédure d'audit analytique** : elle offre de la précision aux preuves, elle a pour but d'aider les auditeurs internes à identifier les éléments qui peuvent entraîner des procédures d'audit complémentaires.

- **Observation** : dans le but d'obtenir une preuve directe d'une situation, et par nature de mode d'obtention, ceci rend la preuve fiable.

- **Echantillonnage statistique** : L'échantillonnage (ou sondage) statistique permet, à partir d'un échantillon prélevé aléatoirement dans une population de référence, dont la taille ne permet pas une analyse exhaustive, d'extrapoler à l'ensemble de la population les observations effectuées sur l'échantillon. Son avantage est d'extrapoler à l'ensemble de la population les observations effectuées sur

l'échantillon, avec une certitude et une précision spécifiée.

- **CAATs : (Computerized Assisted Audit Tools** : extraction / analyse de données) elle permet d'accéder, pour une analyse potentiellement exhaustive, aux données du système informatique de l'organisation. Elle offre une rapidité de mise en œuvre de multiples analyses sur de gros volumes de données.

2. Le rôle de l'audit interne dans l'ERM.

L'un des objectifs fondamentaux de l'audit interne est l'évaluation du processus ERM. Ce dernier peut, selon la culture, le style de management, la taille, la structure et les objectifs de l'entreprise, prendre différentes formes. Et peu importe cette forme, l'audit interne se doit vérifier que les risques significatifs sont couverts. (Groupe Professionnel Industrie et Commerce IFACI, 2003)

Le professeur Mashal a étudié le rôle de l'audit interne dans le processus de management des risques en évoquant deux perspectives différentes : (2012)

2.1. Le rôle de l'AI dans l'ERM selon une perspective Risk Management :

La gestion des risques passe par quatre principales phases qui sont : l'identification et l'évaluation des risques, la hiérarchisation et la planification des réponses aux risques, en plus de la dernière phase de surveillance qui, selon les normes de risques tel que l'IRM 2002, et COSO ERM 2017, doit s'appuyer sur l'audit interne.

The Institute of Risk Management « IRM, 2002 », nous énumère les rôles suivant de l'audit interne par rapport au Risk Management. L'IRM précise que ces rôles peuvent différer d'une organisation à une autre.

Dans la pratique, le rôle de l'audit interne peut inclure tout ou partie des éléments suivants :

- Concentrer les travaux d'audit interne sur les risques significatifs identifiés par la direction, et auditer le processus de management des risques de l'organisation ;
- Fournir une assurance objective sur la gestion des risques ;
- Fournir un soutien actif et une implication dans l'ERM ;
- Faciliter l'identification et l'évaluation des risques, et former le personnel hiérarchique à la gestion des risques et au contrôle interne ;
- Coordonner les rapports sur les risques au conseil d'administration et au comité d'audit.

Lors de la détermination du rôle le plus approprié pour une organisation particulière, l'audit interne doit s'assurer que les exigences professionnelles d'indépendance et d'objectivité ne sont pas enfreintes. (IRM, p. 14)

2.2. Le rôle de l'AI dans l'ERM selon les normes IIA :

L'audit interne doit évaluer l'efficacité des processus de management des risques et contribuer à leur amélioration. (IIA 2120, 2017, p. 20)

Un sondage mené par l'IIA sur plusieurs entreprises a démontré que l'audit interne est fortement impliqué dans le management des risques, sachant qu'il est la troisième ligne de défense contre les risques. Au même niveau que le conseil ou son équivalent. Le rôle clé que joue l'audit interne par rapport à l'ERM, consiste en l'évaluation et l'amélioration de l'efficacité du processus de management des risques, en fournissant, conseils et assurance objective sur l'activité de gestion des risques, au conseil d'administration et à la direction générale, et donner une assurance objective sur le maintien des principaux risques maintenus à un niveau acceptable. (Kertali et Tahajuddiny, 2018)

L'Institut des auditeurs internes, après la parution du cadre COSO ERM, a publié une prise de position, précisément dans les sections 2120, 2120.A1, 2120.A2, 2120.C1, 2120.C2, 2120.C3 et 2210 révisé en 2017, pour clarifier le rôle des audits en ERM.

L'IIA qualifie l'audit interne de fonction indépendante établie au sein d'une organisation dont le rôle est d'évaluer ses activités, et de donner une assurance et des conseils relatives aux domaines de la gestion des risques, du contrôle et de la gouvernance. Plus particulièrement, donner une assurance que les risques sont évalués correctement, en évaluant les processus de gestion des risques ainsi que le reporting des principaux risques et leur gestion.

Selon ce même papier, le rôle de l'audit interne a été classifié en trois types résumés dans cette figure en éventail comme suit :

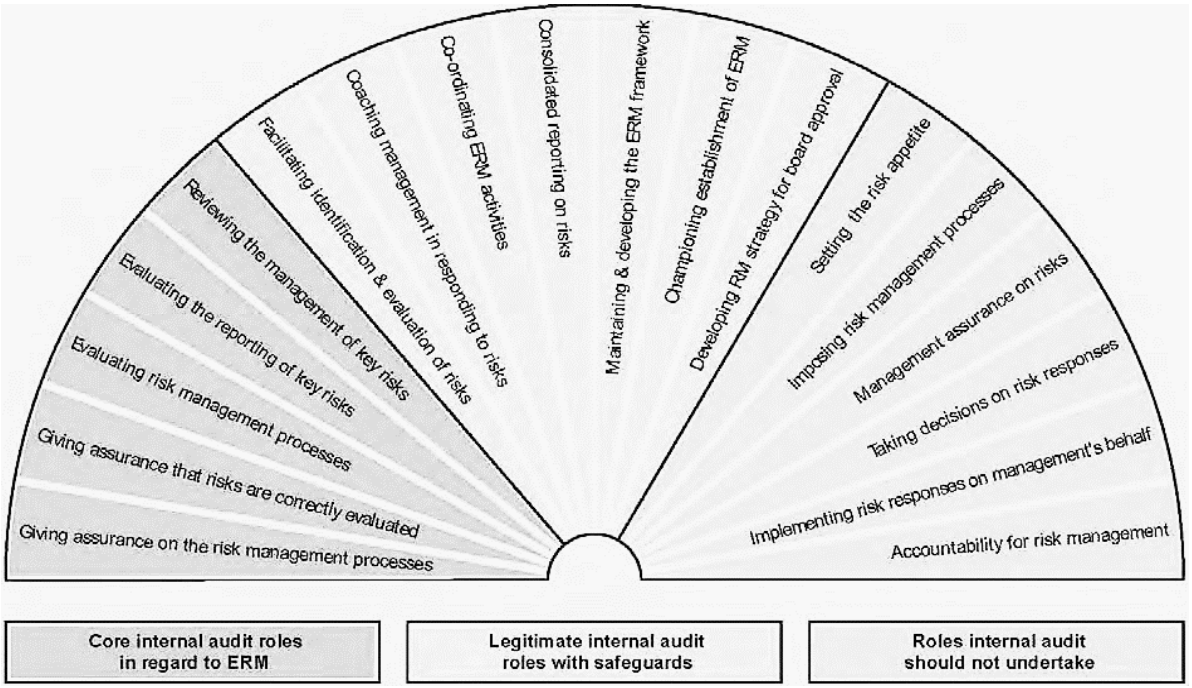


Figure (11) : le rôle de l'audit interne dans l'ERM, à partir de « IIA Position Paper : The Role Of Internal Auditing In Enterprise-Wide Risk Management ». IIA, 2009, p. 4.
https://www.theiia.org/en/content/position-papers/2009/the-role-of-internal-auditing-in-enterprise-wide-risk-management/

On commence la présentation de ces rôles par la gauche de cet éventail jusqu'à sa droite, et on va les présente dans le tableau qui suit :

Typologies des rôles de l'audit interne dans l'ERM	
Principaux rôles de l'audit interne dans le processus de management des risques	- Donner une assurance sur les processus de gestion des risques ; - Donner l'assurance que les risques sont bien évalués ; - Évaluer les processus de gestion des risques ; - Évaluer la communication des risques majeurs ; - Examiner la gestion des principaux risques.
Rôles légitimes de l'audit interne, sous réserve de prendre les précautions	- Faciliter l'identification et l'évaluation des risques ; - Accompagner la direction dans sa réaction face aux risques ;

nécessaires.	- Coordonner les activités de management des risques ; - Consolider le reporting des risques ; - Actualiser et développer le cadre de gestion des risques ; - Promouvoir de la mise en œuvre du management des risques ; - Élaborer une stratégie de gestion des risques à valider par le Conseil.
Rôles que l'audit interne NE doit PAS jouer	- Définir l'appétence pour le risque ; - Définir des processus de gestion du risque ; - Gérer l'assurance sur les risques ; - Décider de la manière de réagir face aux risques ; - Mettre en œuvre des mesures de maîtrise du risque au nom de la direction ; - Prendre la responsabilité de la gestion des risques.

Tableau (05) : Le rôle de l'audit interne dans l'ERM, réalisé par nous-même, inspiré de « IIA position paper : the role of internal auditing in enterprise-wide risk management », IIA, 2006, p. 2 à 3. https://www.theiia.org/en/content/position-papers/2009/the-role-of-internal-auditing-in-enterprise-wide-risk-management/

L'audit interne peut aussi avoir un rôle important dans l'organisation dans le cas où celle-ci ne possède pas d'ERM. Dans cette situation, les missions de l'AI sont diverses : (Groupe Professionnel Industrie et Commerce IFACI, 2003)

- Faire prendre conscience des risques et de l'importance du contrôle interne ;
- Promouvoir la démarche ERM en convaincant la direction générale de constituer un véritable processus de management des risques ;
- Aider l'entreprise à identifier et évaluer les risques au travers d'entretiens avec les principaux managers de l'entreprise qui doivent quantifier l'impact du risque, la probabilité d'occurrence et le niveau de maîtrise ou de contrôle du risque ;
- Gérer et coordonner le processus afin de le faire évoluer et vivre en participant aux comités des risques, aux activités de suivi… sans pour autant être

responsable du Management des Risques.

La maîtrise des risques favorise l'atteinte des objectifs de gouvernement d'entreprise, la création de valeur et le contrôle des dirigeants

Afin de créer ou d'ajouter de la valeur, les auditeurs internes doivent identifier et auditer tout risque éventuel important pour le conseil d'administration et la direction en étendant cette fonction à un audit basé sur les risques. Cette valeur réside dans l'évaluation de l'AI du processus ERM. Car son efficacité conduit à une bonne définition des dispositifs de contrôle interne. (EL Harchaoui, 2019)

En définitive, il incombe à la direction générale et au conseil de déterminer le rôle de l'audit interne dans le processus de management des risques. Leur vision, dans ce domaine, dépendra de facteurs tels que la culture de l'organisation, la compétence de l'équipe d'audit interne, l'environnement culturel local. Cependant, la responsabilité dans le processus de gestion des risques, son impact potentiel sur l'indépendance de l'audit interne nécessitent une discussion approfondie et une approbation de la part du Conseil (IFACI, 2011).

3. Evaluation de l'efficacité d'un processus ERM par l'audit interne

Les normes IIA citées précédemment démontrent que le processus de management des risques doit être évalué comme tout autre processus de l'organisation. Elles attribuent donc une grande responsabilité aux auditeurs internes dans l'évaluation de l'efficacité de ce processus. L'audit interne est donc une fonction essentielle pour toute organisation dans le cadre de l'atteinte de ses objectifs stratégiques et opérationnels, et que les risques significatifs sont identifiés, évalués et traités avec des modalités appropriées et en adéquation avec l'appétence pour le risque de l'organisation tout en assurant une bonne communication relative aux risques entre les membres du management et du conseil d'administration. (E. Sallou, 2019)

Pour J. Verver (2021), un processus ERM efficace doit présenter les caractéristiques suivantes :

- Pilotée par les données extraites de faits réels, et combinées de façon à identifier les tendances et les indicateurs de risque ;
- Dynamique Réactive face aux événements externes et aux évolutions des risques ;
- Fournit continuellement des informations constantes, pertinentes et en temps réel ;
- Exhaustive dans la prise en compte de toutes les formes et les impacts des

risques ;

- Collaborative dans l'assurance du fonctionnement harmonieux des trois lignes de défense ;
- Tournée vers l'avenir en fournissant des notifications de ce qui se passe, de ce qui est susceptible de se produire et de ce qui doit être fait en conséquence ;
- Prend en considération le contexte quand il doit fournir des informations pertinentes pour les responsables à différents niveaux et fonctions, et s'aligne sur les objectifs généraux de l'entreprise ;
- Hautement efficace et pilotée par une technologie conçue spécifiquement pour effectuer tout ce qui précède.

Une gestion des risques efficace dépend d'un processus de management des risques conforme aux politiques et aux normes. C'est pour ça qu'il convient d'auditer ce processus régulièrement afin de vérifier sa conformité et évaluer sa performance dans le but de l'améliorer.

En plus de la dynamicité des organisations qui opèrent dans des environnements tout aussi dynamiques, les changements dans l'organisation et dans l'environnement dans lequel elle opère expliquent la nécessité de surveiller les processus de gestion des risques par des activités de gestion permanente ou par des évaluations spécifiques. (Ferma, 2003)

Plusieurs outils et approches existent pour réaliser ces activités de surveillance et d'évaluation. Nous allons citer trois d'entre elles.

3.1. Approche par principe clés

Cette approche repose sur l'idée que, pour être pleinement efficace, tout processus de
management des risques doit respecter les caractéristiques ou principes minimum requis
par le cadre de référence adopté. (Sallou, 2019)

Dans notre cas on va évaluer l'efficacité de notre processus par rapport à son niveau de conformité aux principes de la norme ISO 31000. Le degré de conformité aux principes clés correspond au degré d'efficacité du processus ERM.

Les principes clés de la norme ISO 31000 qui permettent d'avoir un management des risques efficaces sont les suivants : (IONOS, 2020)

- **Intégré :** le management du risque est intégré à toutes les activités de l'organisme ;
- **Structuré et global :** une approche structurée et globale du management du risque contribue à la cohérence de résultats qui peuvent être comparés ;
- **Adapté :** le cadre organisationnel et le processus de management du risque sont adaptés et proportionnés au contexte externe et interne de l'organisme aussi bien qu'à ses objectifs ;
- **Inclusif :** l'implication appropriée et au moment opportun des parties prenantes permet de prendre en compte leurs connaissances, leurs opinions et leur perception. Ceci conduit à un management du risque mieux éclairé et plus pertinent ;
- **Dynamique :** des risques peuvent surgir, être modifiés où disparaître lorsque le contexte externe et interne d'un organisme change. Le management du risque anticipe, détecte, reconnaît et réagit à ces changements et événements en temps voulu et de manière appropriée ;
- **Meilleure information disponible :** les données d'entrée du management du risque sont fondées sur des informations historiques et actuelles ainsi que sur les attentes futures. Le management du risque tient compte explicitement de toutes limites et incertitudes associées à ces informations et attentes. Il convient que les informations soient disponibles à temps, claires et accessibles aux parties prenantes pertinentes ;
- **Facteurs humains et culturels :** le comportement humain et la culture influent de manière significative sur tous les aspects du management du risque à chaque niveau et à chaque étape ;
- **Amélioration continue :** le management du risque est amélioré en continu par l'apprentissage et l'expérience.

Figure (12) : Principes de la norme ISO 31000 à partir de « ISO 31000 :2018(Fr) Management du risque – Lignes directrices Risk management – Guidelines ». ISO. https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:fr

3.2. Approche par les éléments du processus

Un processus est un ensemble d'activités en interaction qui transforme des éléments d'entrée qui peuvent être des éléments de sortie d'autres processus, en éléments de sortie. Les processus d'un organisme sont généralement planifiés et mis en œuvre dans des conditions maîtrisées afin d'apporter une valeur ajoutée. (ISO 9000, 2015)

Faisant partie des sept principes de la démarche qualité de la norme ISO 9001 version 2015, dont les idées clés sont directement liées à la norme ISO 31000. L'approche processus est une méthode de gestion qui permet de décrire une organisation en identifiant les processus qui regroupent ses grandes activités tel que la direction, la finance, les activités opérationnelles… etc.
L'utilisation de cette approche permettra d'avoir des résultats plus efficaces et efficients. (Certification QSE, s. d).

Il peut y avoir plusieurs processus opérationnels qui se déroulent en parallèle. La

détermination de tous les processus de l'organisme est la première étape de l'approche processus. Ces processus représentés par une cartographie, sont de trois types :

Processus de réalisation	Processus contribuant directement à la réalisation du produit ou du service, depuis la détection du besoin du client à sa satisfaction. Ils correspondent au cœur de métier de l'organisme. Exemples : recherche et développement, conception, fabrication, livraison …
Processus support **(« soutien »)**	Processus qui contribuent au bon déroulement des autres processus en leur apportant les ressources nécessaires. Exemples : maintenance, ressources humaines, maîtrise de la documentation, métrologie …
Processus de management **(« direction »)**	Processus qui contribuent à la détermination de la stratégie, de la politique qualité et au déploiement des objectifs à travers tous les processus de l'entreprise. Ils permettent leur pilotage et la mise en œuvre des actions d'amélioration.

Tableau (06) : Les types de processus pour une approche processus complète à partir de « AXESS QUALITE – l'approche processus » http ://www.axess-qualite.fr/approche-processus.html

Pour le processus ERM, l'adoption de cette approche a pour but d'évaluer l'existence et l'adéquation et la conformité de chaque étape au référentiel choisis, c'est-à-dire l'ISO 31000 dont le processus est composé de cinq phase comme nous l'avons vue dans la section 1, chapitre 2. Pour ce faire nous allons collecter des preuves d'audit en répondant à un questionnaire après avoir mis en place l'approche processus dans l'organisation, identifier le processus à auditer, ses activités sensibles et les risques y afférant. Si des composantes manquent, alors il y a de fortes chances que le management des risques ne soit pas efficace.

Voici ci-dessous des questions exemples permettant de vérifier certains éléments relatifs aux phases du processus ERM : (E. Sallou, 2019)

- **Communication et consultation :** Existe-t-il des échanges structurés et réguliers avec les personnes concernées par les opérations de l'organisation et au sein du secteur d'activité ?

- **Etablissement du contexte :** Les responsables de la gestion des risques

disposent-ils d'une bonne compréhension de l'environnement externe et interne et des activités de l'organisation afin de pouvoir identifier tous les risques ? L'identification des risques est-elle un processus formel et structuré qui tient compte des sources de risques, des domaines d'impact, des événements ainsi que de leurs causes et conséquences potentielles ? L'organisation recoure-t-elle à une technique formalisée pour prendre en compte les conséquences de chaque risque et sa probabilité de survenance ?

- **Appréciation du risque :** L'organisation dispose-t-elle d'un mécanisme permettant de classer les risques en fonction de leurs importance relative, de façon à déterminer l'ordre de priorité dans la mise en œuvre des traitements ?

- **Traitement du risque :** Les décisions concernant le traitement des risques sont-elles rationnelles ?

- **Surveillance et revue :** Un suivi de la mise en œuvre des plans de traitement des risques est-il effectué ? Les contrôles et leur efficacité sont-ils surveillés ? Les activités proscrites sont-elles évitées ? L'évolution du contexte est-elle sans incidence sur les risques ?

3.3. Approche par modèle de maturité

La maîtrise de la complexité d'une organisation et des risques y afférents impose la maîtrise de ses principales fonctions et services. L'optimisation et l'amélioration efficace et efficiente des processus est la clé pour atteindre cette maitrise.

L'évaluation par l'approche « modèle de maturité » du processus ERM permet un examen et une amélioration continue de la performance et de la qualité des ERM. Il existe une multitude de modèles de maturité qui ont été développés par des référentiels tel que la norme ISO/SPICE, la norme ISO 9004 : 2018, CMM… et peu importe le référentiel choisis, la maturité se fond sur cinq niveaux. (Takyorian, 2003)

La mise en œuvre de cette approche nécessite la définition préalable : (E. Sallou, 2019)

- De règles de fonctionnement rédigés sur la base d'une liste d'exigences détaillées, par rapport auxquelles tout progrès dans la mise en œuvre pourra être mesuré ;
- D'un guide sur la manière concrète de respecter les règles et les exigences associées de mesurer les performances effectives au regard de chaque règle et de chaque exigence ;

- D'outils capable d'enregistrer les performances et progrès tout en les soumettant à des vérifications périodiques des évaluations déjà effectués par le management.

Le CMMI (Capability Maturity Model Integration) développé par le SEI, Software Engineering Institute de l'Université Carnegie Mellon, est le plus souvent utilisé car il offre un cadre d'évaluation et d'amélioration de la maitrise des processus techniques et managériaux.

Ce modèle est une référence internationale de cinq niveaux, qui permet d'évaluer la maturité d'un processus dans l'objectif de l'améliorer en identifiant les caractéristiques devant être satisfaits par le processus pour lui permettre de passer à un niveau supérieur de maturité. Ces niveaux sont représentés dans le tableau ci-dessous : (Carlier, 2006)

Niveaux		Concepts.
1	Initial/ Naïf	Le processus est immature ou bien n'existe même pas. La cuture du risque n'est pas développée. Les standards de travail sont absents, et les principes de la gestion du risque sont mal, voire pas du tout appliqués.
2	Reproductible/ Réactif	Le processus existe, il est opérationnel. Mais son bon fonctionnement est basé uniquement sur l'expérience acquise et le savoir-faire et non sur les standards.
3	Défini/ Standard	Le processus est formalisé, standardisé, définis et documenté, normalisé et compris. Il est suivi et contrôlé dès sa mise ne place.
4	Maitrisé/ Proactif	Le processus est formel, bien compris et maitrisé. La prévention des risques est bien assurée, et les objectifs préétablis sont atteints.
5	Optimisé/ Amélioratif	Le processus est optimisé en permanence et toutes les évolutions et les développements sont maîtrisés. La gestion des risques est en constante amélioration qui l'engagement et la participation de l'ensemble des collaborateurs.

Tableau (07) : les niveaux de maturité du CMMI, fait par nous-même, inspiré de « Management de la qualité pour la maîtrise du SI », A. Carlier, 2006, p. 182, LAVOISIER

Conclusion

L'intention derrière ce chapitre était de présenter ce qu'un processus de management des risques, et de mettre la lumière sur le rôle de l'audit interne dans l'amélioration de l'efficacité de ce dernier. Pour ce faire nous avons deviser notre travail en trois sections.

Dans la première nous avons dressé un exemple de processus de management des risques inspiré de la norme ISO 31000 « Risk Management ». Ce qui nous a permis de comprendre qu'un cadre de management des risques complet, accompagné d'un processus ERM respectant les normes améliore le reporting des risques et permet d'identifier les principaux risques susceptibles d'affecter l'organisation, il peut également améliorer la productivité et la conformité.

Pour la deuxième section, nous avons essayé d'expliquer la relation entre le contrôle interne et un processus ERM. Puis de mettre en évidence l'importance de jumeler ces deux fonctions afin de mieux gérer, de minimiser et, dans certains cas, d'éliminer les risques, afin de préserver la sécurité et l'activité de votre entreprise.

Et enfin nous avons évoqué dans la troisième section, l'importance d'évaluer le processus ERM par l'audit interne. Cette évaluation aide les organisations à améliorer l'efficacité de leurs processus de management des risques. Car après tout, le rôle clé de l'audit interne est de fournir une assurance au management et au conseil sur la gestion des risques et en même temps sur l'efficacité du processus ERM.

L'ERM est un processus structuré, cohérent et continu, appliqué à l'ensemble de l'organisation. Appliqué convenablement il permet d'identifier et d'évaluer les risques, ainsi que de décider des réponses à apporter aux opportunités et menaces qui affectent la réalisation des objectifs, et d'en rendre compte. C'est pour cela que l'IIA insiste sur l'implication de l'audit interne dans le management des risques, et principalement dans l'amélioration du processus concerné.

CHAPITRE 3 :

Evaluation du processus de management des risques, cas de la B.N.A

Introduction

Les deux précédents chapitres consacrés à l'aspect théorique de notre travail, nous a permis dans un premier temps, de prendre connaissance de la notion de système d'information, son importance dans une organisation, et la nécessité de gérer les différents risques opérationnels que peut engendrer un SI, afin de préserver sa sécurité et son activité.

Dans le second chapitre nous avons démontré l'importance d'avoir un processus de management des risques adhérant aux normes, et qui aidera l'organisation à gérer, à minimiser et voir même, à éliminer les risques. Nous avons terminé par mettre le point sur le rôle important que peut jouer l'audit interne dans l'amélioration de ce processus.

Dans la volonté de vérifier nos hypothèses issues de notre problématique, et dans le but de répondre à nos questions secondaires, nous nous somme diriger vers la Banque Nationale d'Algérie
« B.N.A » afin de récolter les données nécessaires à notre travail.

Ce dernier chapitre sera consacré à la présentation générale de la B.N.A, ainsi que ses fonctions d'audit interne et de gestion des risques. Puis après avoir expliqué notre méthodologie de travail, nous allons analyser et interpréter les différentes données recueilles afin d'en tirer une conclusion, et peut être une réponse à notre problématique

Section 1 : présentation de la Banque Nationale d'Algérie B.N.A

Notre intérêt est focalisé dans cette section sur la présentation de la Banque Nationale d'Algérie et ses différentes directions concernées. Nous avons commencé par la présentation de la BNA de manière générale, ensuite nous avons présenté les missions et l'organisation de la Direction de l'Audit Interne de la banque. Nous avons également exposé et traité l'organisation de la gestion des risques au sein de la banque.

1. Historique de la B.N.A

Créée le 13 Juin 1966, la Banque Nationale d'Algérie est la première banque commerciale en Algérie, reprenant les activités algériennes du Crédit Foncier d'Algérie et de Tunisie.

Etant une société par action au capital de 150.000.000.000 DA, dont le siège social se trouve à Alger, 8 boulevard Che Guevara, la B.N.A a été, en Septembre 1995, la première banque algérienne à obtenir son agrément conformément aux dispositions de la loi 90-10 relative à la Monnaie et au Crédit. Elle exerçait dès lors toutes les activités d'une banque universelle et elle était chargée en outre du financement de l'agriculture.

En 2013, la BNA annonce un résultat net bénéficiaire de 30,2 milliards de dinars algérien, et au mois de juin 2018, le capital de la BNA est passé de 41,6 milliards de dinars algérien à 150 milliards de dinars algérien.

La BNA gère en 2015 plus de 2 513 197 comptes clientèles, et un réseau de 43 agences réparties sur tout le territoire algérien, 6 directions de réseau d'exploitations et distributeurs automatiques de billets 90 guichets automatiques de banque, plus de 5 000 collaborateurs. Elle a élargi son réseau et a mis à la disposition de sa clientèle 221 agences, implantées sur le tous le territoire national, chapotées par 20 Directions régionales.

Pour le développement de la monétique, la BNA délivre gratuitement à sa clientèle des cartes CIB, leurs facilitant ainsi au quotidien la réalisation de leurs opérations diverses à travers l'implantation de 98 Guichets Automatiques de Banque et 150 Distributeurs Automatiques de Billets. (Le site de la B.N.A, www.bna.dz)

1.1. Composition du réseau de la B.N.A

La Banque Nationale d'Algérie comporte : (Le site de la B.N.A, www.bna.dz)

- 221 Agences réparties sur tout le territoire national,
- 20 Directions de Réseau d'Exploitations.
- 151 Distributeurs Automatiques de Billets.
- 100 Guichets Automatiques de Banque.
- Plus de 5000 Collaborateurs.
- Plusieurs centaines d'entreprises abonnées au service.
- 278 315 Cartes Inter Bancaires.
- 2 944 174 Comptes Clientèles.
- 45428 Clients Abonnés en E-Banking.
- 5221 Terminal de Paiement Electronique installés.
- 13 web marchand

1.2. Structure organisationnelle de la B.N.A

Rattachements	Structures	Rattachements	Structures
La direction générale	- Secrétariat général - Direction de l'organisation des méthodes et procédures - Direction de la conformité et direction de communication - Inspection générale et la direction d'audit interne	**La division systèmes d'information**	- Direction de la Production et des Services - Direction des Technologies et de l'Architecture - Direction du Développement Etudes et Projets
		La division internationale	- Direction des Mouvements Financiers avec l'Etranger. - Direction des relations internationales et du commerce extérieur - Direction des Opérations Documentaires.
La division stratégie et développement	- Direction de la Stratégie et Management de Projets et Direction du Développement des Performances. - Direction du Développement des Talents et Direction des Filiales et Participations.	**La division financière**	- Direction des Marchés Financiers et direction de la comptabilité - Direction du Contrôle de Gestion - Direction des Reporting Comptables Légaux et Réglementaires
La division engagement	- Direction des Grandes Entreprises. - Direction des Petites et Moyennes Entreprises. - Direction de Crédit aux Particuliers et Spécifiques. - Direction de l'Administration et du Suivi des Crédits	**Division risques et contrôle permanent**	- Direction de contrôle Permanent. - Direction de la Gestion des Risques et Cellule de Sécurité SI
La division exploitation et action commerciale	- Direction de L'Encadrement du réseau. - Direction de l'Animation Commerciale.	**La division gestion des moyens matériels et RH**	- Direction des Ressources Humaines et Direction de la Formation. - Direction des Moyens Généraux.

			- Direction de la Préservation du Patrimoine. - Direction du Développement du Patrimoine Immobilier. - Centre de Gestion des Œuvres Sociales.
La division recouvrement, études juridiques er contentieux	- Direction des Etudes Juridiques et du Contentieux - Direction de Recouvrement des Créances. - Direction Etudes, Validation et Suivi des Garanties	**La division finances islamiques**	- Direction d'Exploitation Islamique. - Direction Financière, Contrôle et Gestion des Risques Islamique. - Direction Animation Commerciale et Ressources Humaines Islamique.
La division digitalisation, marketing et paiement	- Direction Marketing et Innovation - Direction de la Monétique et direction des instruments de paiement	**La division stratégie et développement**	- Direction d'Exploitation Islamique. - Direction Financière, Contrôle et Gestion des Risques Islamique. - Direction Animation Commerciale et Ressources Humaines Islamique

Tableau (08) : Structure organisationnelle de la B.N.A, fait par nous-même à partir de www.bna.dz

1.3. Missions et services de la B.N.A

Une banque de manière générale a pour mission de recevoir les dépôts du public, collecter l'épargne, fournir et gérer les moyens de paiement et accorder des prêts. Pour se faire la B.N.A a mis à disposition de sa clientèle toutes une panoplie de produits et services bancaires ainsi que des produits d'assurance, destinés à satisfaire toute sa clientèle. www.bna.dz

Formules de financement	**Crédits à la consommation**	Cette formule est faite pour ceux qui souhaitent acquérir un véhicule, de l'immobilier ou tout autre bien à grande valeur. Composés de deux solutions, crédit CONFORT et crédit AUTO, qu'on peut fusionner grâce à leur flexibilité, et un taux d'intérêt et des avantages concurrentiels.
	Crédits immobiliers	La B.N.A offre onze formules pour ceux qui souhaites acheter ou faire une extension de leur logement. On peut citer le crédit pour l'aménagement d'une habitation avec un taux d'intérêt concurrentiel de 6,25% pour les non épargnants.
	Crédits spécifiques	Ce servies est fait pour les chômeurs et les nouveaux diplômés qui veulent se lancer dans l'entreprenariat. On Trouve trois formules de crédit avec les établissements ANGEM, ANSEJ et CNAC.
	Crédits à long terme	C'est un crédit d'une durée de plus de 7 ans destiné au financement de gros investissements, tels que la construction des infrastructures et l'acquisition d'équipements, avec une période de différé de paiement adaptée à votre activité pouvant atteindre 05 ans.
	Crédits à moyen terme	La BNA met à disposition ce crédit pour une durée allant de 2 à 7 ans avec une période de différé de paiement adaptée à l'activité allant de 01 à 03 ans
	Crédit-bail	C'est un moyen de financement des investissements de biens d'équipements et de matériels sans affecter la capacité d'emprunt, il permet d'économiser sur les impôts à payer. Sa durée est égale à la durée d'amortissement, avec une option d'achat à la fin du contrat
	Crédits par signature	Il est fait pour l'importation de biens, soumissions qui nécessitent des cautions...etc. La BNA se porte garante par sa signature.
	Crédits par caisse	Ils sont à court terme est sont sous forme de facilité de caisse, escompte du papier commercial, le découvert et avance sur marché.

Epargne	**Dépôts à terme**	C'est un placement rémunéré pour une durée déterminée allant de 3 à 120 mois, il peut être en dinars ou en devises. Montant minimum : 10 000 DA.
		La BNA offre la possibilité de placer une épargne avec la formule « BON DE CAISSE » anonyme, normatif ou porteur, pour une durée allant de 3 à 120 mois et des coupures variables au choix. Montant minimum 10.000 DA.
	Dépôts à vue	Cette épargne marche avec un livret d'épargne qui peut être au choix, avec ou sans intérêt. La B.N.A a aussi, en plus des comtes « Epargne Plus » au taux évolutif allant de 2,5% à 4,5% l'an, des livrets d'épargne junior « MOUSTAKBALY » pour les enfants de 0 à 15 ans
Commerce extérieur	La B.N.A, accompagne les importateurs et exportateurs dans le montage, la négociation et la réalisation de leurs opérations avec l'étranger. Grâce à son réseau domestique, ses correspondants bancaires, ses filiales et participations en Algérie et à l'étranger, elle offre à ses clients la pré domiciliation, des crédits documentaires, des garanties internationales, des remises documentaires, des virements internationaux et des exportations hors hydrocarbures.	

Tableau (09) : les différents produits et services de la B.N.A, réalisé par nous-même à partir de www.bna.dz

2. Présentation de la fonction d'audit interne de la B.N.A

La fonction de l'audit interne de la BNA a été créé le 26 Février 1995 sous forme d'une cellule rattachée hiérarchiquement et administrativement à l'inspection générale. Ses missions et son organisation ont été définis le 23 Novembre 1995 via une circulaire.

Le 28 Décembre 2006, elle est devenue une direction rattachée directement au président directeur général à ce jour. Ce qui lui a permis de se doter de prérogatives et pouvoirs nécessaires à l'accomplissement de ses missions.

La charte d'audit de la BNA qui couvre l'ensemble des activités et des fonctions de la DAI, précise que l'audit interne est un dispositif permanent et indépendant, qui a pour mission d'évaluer l'efficacité du système de contrôle interne, et de l'ensemble des processus.

2.1. Missions de la DAI

La Banque Nationale d'Algérie a défini les missions de sa direction de l'audit interne via une circulaire interne, les principales missions sont :

- Accroitre et de préserver la valeur de la banque, en donnant avec objectivité une assurance, des conseils et des points de vue fondés sur une approche par les risques.

- Evaluer, par une approche systémique et méthodique de la qualité du système de contrôle interne et les processus de management des risques.

- Formuler les recommandations appropriées, pour une valeur ajoutée reconnue, destinée à optimiser le système de contrôle interne.

- Communiquer à la Direction Générale, au Comité d'Audit et aux destinataires appropriés le résultat de ses missions.

- Suivre la prise en charge effective des recommandations.

2.2. Organisation de la DAI

La DAI est composée d'équipes constituées d'Auditeurs Seniors, Auditeurs et Auditeurs Juniors et d'un service « Gestion Administrative », qui sont chapotés par un directeur.

2.2.1. Le directeur d'audit interne

Son statut lui permet de diriger, de coordonner, et de répartir les tâches, les fonctions, les activités et les missions de la structure dont il est responsable.

Le directeur d'audit interne élabore et exécute les plans d'action et les rapports d'activité de la direction, conformément au plan d'action préalablement arrêté et approuvé par la direction générale dans le cadre des prérogatives et règlements en vigueur. Il veille aussi à la formation du personnel de sa direction.

Il est chargé aussi :

- D'élaborer les méthodes de travail de la direction ;

- De suivre la réalisation des missions d'audit arrêtées ;
- De valider les missions conduites par les auditeurs ;
- De présenter les rapports et les synthèses sanctionnant les missions réalisées à la DG ;
- De rendre compte au CA, de l'exécution du plan d'action à la fin de chaque semestre ;
- De communiquer au CA, sur sa demande, les éclaircissements et les détails jugés importants relatifs au programme annuel et au rapports d'audit ;
- De veiller au suivi de la mise en œuvre des recommandations issues des missions d'audit ;
- D'intervenir sur des missions d'audit stratégiques ou sur des dossiers présentant des spécificités.

2.2.2. Auditeurs et auditeurs seniors

L'auditeur senior a pour rôle de piloter, d'animer et de suivre les travaux de missions qui lui sont confiées et de s'assurer de leur achèvement dans les délais. Il est l'interlocuteur avec le responsable de la DAI et les audités.

A ce titre, il a pour tâches essentielles :

- D'intervenir dans la préparation et la planification des missions ;
- D'affecter les travaux aux auditeurs ;
- De suivre l'avancement des travaux ;
- De valider les travaux réalisés par les auditeurs ;
- D'élaborer le compte rendu de mission, le rapport final et la synthèse y afférents ;
- D'assurer le suivi de recommandations ;
- De participer dans la préparation du plan d'action et des rapports périodiques ;
- De contribuer à l'enrichissement des projets de textes organiques soumis à la DAI.

Quant à l'auditeur, son rôle consiste à participer à des missions d'audit en vue d'évaluer le niveau et la maitrise des risques et l'efficacité des dispositifs de contrôle. Il a pour principales tâches de réaliser les travaux qui lui sont confiés par le chef de mission et de participer à l'accomplissement des tâches dévolues à l'auditeur sénior. En ce qui concerne l'auditeur junior, son rôle est de contribuer à la réalisation des travaux confiés aux auditeurs.

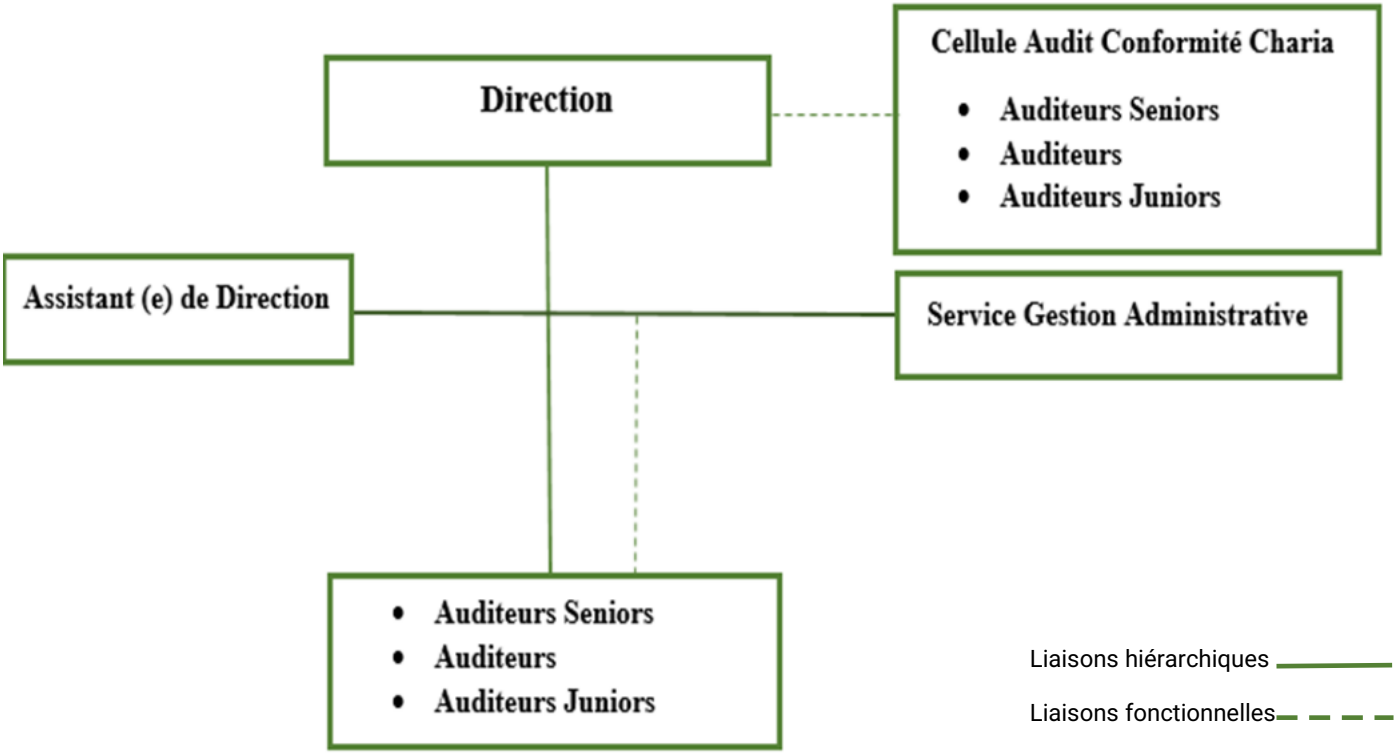
2.2.3. Le service gestion administrative

Ce service, selon les documents internes de la BNA, a pour mission principale d'assurer la gestion des moyens humains et matériels de la direction ainsi que la cellule Audit de conformité Charia. Le chef de ce service est chargé de :

- Veiller à la discipline générale et au respect du règlement intérieur de la banque ;
- Gérer les dossiers administratifs du personnel ;
- Suivre les plans de formation initiés au profit du personnel ;
- Elaborer et de suivre le planning des départs en congé du personnel ;
- Contrôler et de mandater les relevés des frais de missions du personnel ;

- Elaborer le budget et de suivre périodiquement les réalisations budgétaires ;
- Passer les commandes de fournitures et consommables et faire le suivi des livraisons ;
- Gérer l'économat ;
- Assurer la bonne exécution des écritures comptables ;
- Arrêter la journée comptable et d'établir les différents états ;
- Suivre et de mettre à jour les fichiers d'inventaire physique du matériel et du mobilier de la DAI et de la cellule Audit de Conformité Charia et procéder au rapprochement des inventaires physico-comptables avec les services concernés de la banque ;
- Assurer la gestion des abonnements et le règlement des factures (redevances, consommations…) ;
- Assurer la bonne tenue des registres légaux ;
- Assurer la logistique et le règlement des frais à l'occasion de tenue de réunions du CA.

Figure (13) : l'organigramme de la direction d'audit interne de la B.N.A, à partir de la documentation interne de la banque, 2021.



2.3. Les missions d'audit interne au sein de la B.N.A

L'audit interne couvre l'ensemble des activités et des fonctions de la banque conformément à la politique générale définie par l'organe dirigeant. La circulaire interne de la banque définit l'audit interne comme :

Une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maitrise de ses opérations, lui apporte ses conseils pour les

améliorer, et contribue à créer de la valeur ajoutée. Il aide cette organisation à atteindre ses objectifs en évaluant, par une approche systémique et méthodique, ses processus de management des risques, de contrôle, et de gouvernance, et en faisant des propositions pour renforcer leur efficacité. (2021)

La DAI est dotée de prérogatives et pouvoirs nécessaires à l'accomplissement de ses missions, qui sont bien expliqués dans sa circulaire interne. La nature des interventions de l'audit interne est définie comme suit :

- **L'audit d'efficacité :** qui porte sur le contrôle de la qualité et la pertinence des procédures mises en place pour garantir la conformité aux lois, règlements et à la politique de la banque.
- **L'audit opérationnel :** il réside dans le contrôle de la qualité et de la pertinence des systèmes et des procédures, l'évaluation de l'adéquation des ressources et méthodes aux objectifs assignés et l'analyse des structures et de l'organisation en exerçant un esprit critique.
- **L'audit de procédures** : il consiste à contrôler l'application et l'efficacité des procédures notamment de management des méthodes de mesures des risques.
- **L'audit comptable et financier** : il s'appuie sur la vérification de la sincérité et de la fiabilité des procédures comptables, des enregistrements comptables et des états financiers qui en résultent.
- **L'audit des systèmes d'informations :** il porte sur le contrôle des systèmes d'informations et comptables.
- **L'audit réglementaire :** il consiste à contrôler les dispositifs mis en place pour s'assurer qu'ils sont conformes aux exigences légales et réglementaires ainsi que le contrôle de sincérité, de fiabilité et d'opportunité des reporting réglementaires.
- **L'audit de management :** il concerne l'évaluation de la qualité de l'approche du risque et du contrôle interne par les managers dans le cadre des objectifs de la banque.

La DAI est placée sous l'autorité directe du Directeur Général, elle est dirigée par un directeur qui relève hiérarchiquement de ce dernier. Son champ d'activité, d'après le document interne de la banque, couvre l'ensemble des structures de la banque avec lesquelles elle entretient des relations fonctionnelles et de coopération et plus particulièrement avec :

- Le comité d'audit « CA ».

- L'inspection générale.
- La division risques et contrôle permanent. « DRCP »
- La direction du contrôle permanent. « DCP »
- La direction de la gestion des risques « DGR ».
- La direction de la conformité
- La cellule sécurité des systèmes d'informations « CSSI ».

La direction de l'audit interne entretient également des relations avec les différents partenaires externes et les commissaires aux comptes.

3. La division risques et contrôle permanent

Placée sous l'autorité du directeur général, la division risques et contrôle permanant représente la structure hiérarchique et coordinatrice de la direction du contrôle permanent « DCP », la direction de la gestion des risques « DGR », et la Cellule Sécurité des Systèmes d'Information.

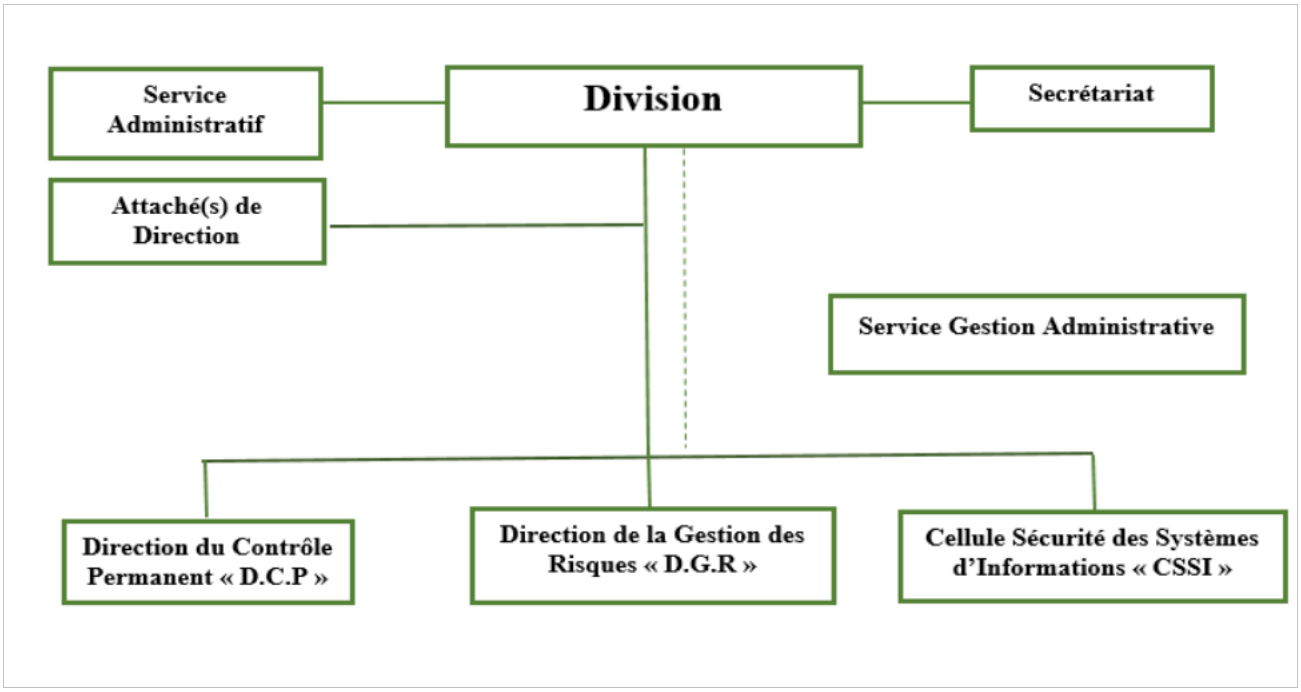
Créée et mise en place le 23 septembre 2019, conformément aux exigences réglementaires de la loi 11-08 de la Banque d'Algérie relative au contrôle interne des banques et établissement financiers, la DRCP exerce une autorité fonctionnelle sur l'ensemble des structures de la banque pour ce qui a trait à son domaine d'activité. (Documents internes de la BNA, 2022)

3.1. Organisation de la DRCP

Pour assurer ses missions, la DRCP est composée de :

- **Le chef de la division** : il dépend hiérarchiquement du DG auquel il rend compte de l'activité de la division et des structures rattachée. Il est chargé de l'élaboration des plans d'actions et des budgets se rapportant à son domaine d'activité. Il assure la coordination entre les structures placées sous son autorité, et celle des dispositifs de contrôle permanant.

- **Les attachés de direction** : qui sont chargés de l'étude et de l'analyse des dossiers qui leurs sont confiés. Ils effectuent également une consolidation des plans d'actions des structures rattachées à la division, en tenant compte des objectifs qui leurs sont assignés.



- **Le service administratif :** chargé d'assurer le suivi et l'exécution des textes et procédures en vigueur, de toutes les tâches administratives et comptables inhérentes aux activités de la division. Il gère également les dossiers administratifs du personnel de la division et tient un dossier miroir des structures rattachées.

- **Le secrétariat.**

Figure (14) : l'organigramme de la division risques et contrôle permanent de la B.N.A, à partir de la documentation interne de la banque.

3.2. La direction gestion des risques

La maitrise des risques liés au développement de l'activité bancaire, en application du règlement Banque d'Algérie n°11-08, impose la création d'une organisation de gestion des risques, dont la finalité est de neutraliser les risques de

crédit, les risques financiers et les risques opérationnels.

La direction de gestion des risques a pour mission principale l'identification, l'évaluation et la surveillance des risques de la banque, et elle s'occupe aussi de :

- Définir les méthodes et les outils de maitrise et de couverture des risques.
- Définir les procédures relatives aux différents risques.
- Veiller au respect et à l'ajustement des limites fixées des différents risques suivant 1'évolution de l'activité de la banque.
- Elaborer les rapports périodiques, portant sur le résultat des travaux menés relatifs à l'exposition de la banque aux risques et sur les mesures d'actions à prendre.
- Elaborer et actualise périodiquement la cartographie des risques opérationnels et communique les résultats aux organes de la banque.
- Mettre à disposition des responsables du contrôle permanent et du contrôle périodique les fichiers des incidents significatifs.
- Veiller à l'examen de l'évolution de la qualité du portefeuille crédit global et communique les résultats aux organes de la banque.
- Veiller à l'analyse des états reporting reçus des différents risques.
- Elaborer un rapport semestriel et annuel sur la mesure et la surveillance des risques de la banque en coordination avec l'ensemble des structures de la banque.

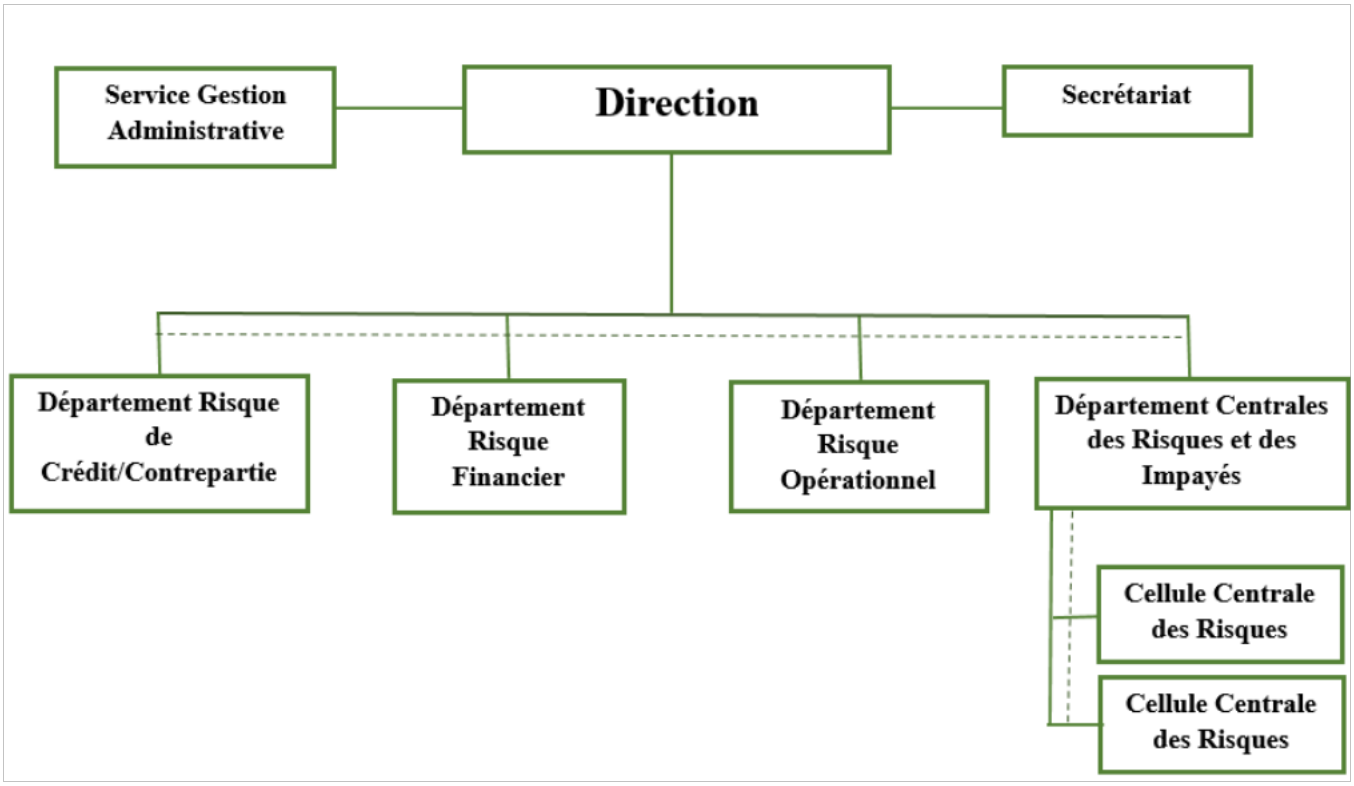
3.2.1. Organisation de la DGR

La Direction de la Gestion des Risques est structurée en quatre départements et un service. (Documents interne de la BNA)

- **Département Risques de Crédit/Contrepartie :** il a pour principale missions le pilotage, l'animation, la coordination en matière de gestion, d'analyse et de suivi des risques de crédit.

- **Département Risques Financiers :** composé d'un chef et de contrôleurs et des chargés d'études, ce département entretient des relations fonctionnelles étroites avec la Direction des Marchés Financiers et la Direction Animation Commerciale.

  Il a pour principale missions le pilotage, l'animation, la coordination en matière de gestion, d'analyse et de suivi des risques notamment les risques interbancaires, les risques de liquidité, les risques de taux d'intérêt…etc.



- **Département Risques Opérationnels :** il a pour principale mission le pilotage, l'animation, la coordination en matière de gestion, d'analyse et de suivi des risques opérationnels.

- **Département centrale des Risques et des Impayés :** il a pour mission la gestion de la centrale des impayés, composé de deux cellules, une des risques, et l'autre des impayés.

- **Service Gestion Administrative** : il a pour principale mission d'assurer le suivi et l'exécution, dans le strict respect des textes et procédures en vigueur, de toutes les tâches administratives et comptables inhérentes aux activités de la direction.

Figure (15) : organigramme de la direction gestion des risques de la B.N.A, à partir de la documentation interne de la banque.

3.3. La cellule sécurité des systèmes d'information

Rattachée directement à la division des risques et contrôle permanent, et complétement indépendante de la DSI. La cellule sécurité des systèmes d'information a été créée et mise en place le 03 Octobre 2019, conformément aux exigences réglementaires de la loi 11-08 de la Banque d'Algérie relative au contrôle interne des banques et établissement financiers, dans le but de s'occuper de la sécurité des systèmes d'information.

La CSSI exerce une autorité fonctionnelle sur l'ensemble des structures de la banque pour tout ce qui a trait au domaine de la sécurité des systèmes d'information., et elle entretient notamment des relations fonctionnelles et de coopération avec ces structures.

3.3.1. Organisation de la CSSI

Composée d'ingénieurs en informatique ayant acquis une expérience confirmée dans le domaine, cette cellule est dirigée par un responsable nommé par la décision du Directeur Général qui est chargé de :

- La conception du programme d'activité de la cellule ;
- L'exécution, la coordination ainsi que la supervision des travaux de son entité ;
- L'élaboration des rapports semestriels et annuels de l'activité de la structure, ainsi que les divers rapports de synthèse à transmettre à la Direction Générale ;
- L'établissement du bilan des différentes interventions réalisées par la cellule.

Section 2 : méthodologie de l'étude

La revue de littérature nous a permis de dresser le cadre théorique de notre étude. Ce cadre théorique ainsi dressé servira de levier pour l'élaboration de la méthodologie à suivre pour atteindre les objectifs de l'étude. Il sera question pour nous maintenant, d'élaborer le modèle d'analyse, de présenter les outils de collecte et d'analyse des données

L'étude menée au niveau de la B.N.A s'est appuyée sur trois outils de collecte et d'analyse des données, qui sont liés entres elles.

1. L'analyse documentaire

Une méthode qui consiste à exploiter les différents documents de la B.N.A, sur les différents lieux de travail, afin d'avoir une connaissance générale sur le fonctionnement de celle-ci. Les différentes informations collectées de cette analyse seront complétées par des entretiens.

2. Interviews

L'interview est un entretient avec une personne en vue de l'interroger sur ses actes, ses idées …etc. Cette technique nous permettra de disposer des éléments d'analyse et d'orientation dont nous avons besoin afin d'avancer la recherche de notre mémoire.

Nous avons opté pour le mode d'administration face à face avec les différents directeurs et responsable concernés, à savoir le directeur de l'audit interne de la BNA, le directeur de la gestion des risques ainsi que la responsable du département risques opérationnels, la responsable de la division risque et contrôle permanant, et la responsable de la cellule sécurité des SI.

3. Le questionnaire

Le questionnaire est un outil indispensable et un élément essentiel pour la réalisation de l'enquête, il permet de recueillir des informations relatives aux activités du répondant. C'est un ensemble de questions construites dans le but de générer l'information nécessaire à l'accomplissement d'une étude.

Composé de vingt-sept questions, réparties sur deux parties, une première concernant le cadre organisationnel de la gestion des risques SI, et une autre sur la prise de connaissance de leur processus de management des risques. Les questions figurant

dans notre questionnaire sont de différentes formes (questions fermées à choix unique, questions fermées à choix multiple, questions ouvertes).

Nous l'utilisons dans le but de disposer de renseignements, nous permettant de comprendre le fonctionnement de l'organisation, de son dispositif de management des risques, de l'audit interne et son apport à ce dispositif.

Section 3 : interprétation des résultats

Durant notre stage au sein de la Banque Nationale d'Algérie, nous avons pu, malgré la contrainte de confidentialité et de manque d'informations, avoir une idée sur la fonction de management des risques, la fonction d'audit interne, ainsi que son apport à l'amélioration du processus de managent des risques opérationnels liés aux systèmes d'information.

1. Cadre organisationnel de la gestion des risques SI au sein de la B.N.A

Introduite grâce à l'ancienne direction général, le risque est une notion récente dans l'organisation, tout comme la division risques et contrôle permanent qui est encore dans un état embryonnaire. Ce qui n'a pas empêcher les agents de la BNA et plus particulièrement les opérationnels et les agents de réseaux d'avoir une culture du risque assez présente.

Grâce aux directives de la loi 11.08 du 28 novembre 2011 de la banque d'Algérie, la BNA a pu cerner ce qu'un risque (Article 2, paragraphe i, p.03), quels sont ses types, et l'importance de la mesure et d'analyse du risque opérationnel (Article 27 de la loi 11.08)

1.1. La fonctions gestion des risques de la BNA

Etant un objectif majeur de la DG, la gestion des risques a pris une place importante parmi les objectifs managériaux de l'organisation. Ce qui s'est traduit par la création d'une division complétement indépendante, ce qui est une première parmi toutes les banques d'Algérie.

1.1.1. Les objectifs de la BNA en gestion des risques

Ces derniers sont définis, mis à jour et distribués sous forme de plants d'actions pour chaque division, direction et cellule. Parmi eux on trouve :

- La mise en place d'un plan de continuité d'activité qui est en cours de validation, pour palier au risque de disponibilité du SI ;
- La mise en place d'une politique de sécurité des systèmes d'information PSSI, qui est mise en place et validé par la DG en 2021. Ce PSSI comporte toute un chapitre sur la gestion des risques opérationnels liés aux SI, et décrit les principaux risques tel que la confidentialité et la disponibilité du SI ;
- La création d'une cellule pour la sécurité des SI « CSSI » qui est directement rattaché à la DRCP, et indépendante par rapport à l'opérationnel. Ce qui lui permet de garder un œil sur les activités de la DGR et de la contrôler. Cette cellule est créée en réponse l'envie de réponde à l'objectif de la gestion des risques SI qui est en permanence abordé étant donné son importance, et permettre d'identifier les principaux risques.

  La DRCP qui est directement rattaché à la direction général grâce à son statut de division à toutes les qualifications nécessaires pour exercer une certaine notoriété sur les opérationnels et les dirigeants.

1.1.2. La définition des responsabilités en la gestion des risques

La BNA a recours à des circulaires propres à chaque division et direction. Dans ces circulaires on trouve les responsabilités de chaque intervenant de près ou de loin dans la gestion des risques.

Ces responsabilisées concernent particulièrement la gestion de trois principaux risques qui sont les risques de marché, les risques de crédit et les risques opérationnels.

Ces circulaires sont en constante amélioration, la dernière mis à jour était celle de la circulaire n° 2277 du 15 Juillet 2020.

Actuellement la direction de la BNA est entrant de détailler les procédures qui concernent la politique de gestion des risques opérationnels et de la sécurité des SI.

1.1.3. Les obligations légales et règlementaires applicables en matière de communication sur les risques

Au niveau externe, la BNA suit les directives de la Banque d'Algérie en ce qui concerne la communication sur les risques. Notamment règlement n°2014-02 du 16 Février 2014 relatif aux grands risques et aux participations, qui exige de tout organisme financer de :

- Soumettre un rapport annuel sur la surveillance et la maitrise des risques en suivant la méthodologie énoncée dans ce même règlement ;

- Déclarer le taux des ratios liés aux risques opérationnels et ceux de l'endettements et de solvabilité, en plus des scénarios sur les risques de crédit ;

- Remplir chaque trimestre, des états récapitulatifs fournis par la BA sur la gestion des risques. Cette tâche est réalisée par la direction des Reporting Légaux Et Réglementaires « DRLR ».

Au niveau interne, la DCP se doit d'emmètre des rapports semestriels sur le contrôle interne concernant les divisons risques, engagements, marchés financiers et la division comptable.

La DRCP a même créée un comité sécurité système d'information « CSSI » afin de communiquer sur les démarches à entreprendre vis-à-vis du risque, mais aussi communiquer avec le comité d'audit

2. Evaluation des risques opérationnels lié au SI

Comme nous l'avons vue dans la théorie (chapitre 1, section 3, point 3), la DSI est, dans la plupart des cas responsable de la gestion des risques SI. Mais pour la BNA cette direction n'est qu'une structure support pour son système d'information.

La DSI ne s'occupe que de mettre à la disposition des SI, en plus du hardware, des applicatifs. C'est-à-dire des logiciels et des programmes permanant d'effectuer des tâches précises, tel que la gestion des comptes bancaires grâce à des logiciels sophistiqués, permettent par exemple, de faire des virements en ligne et de gérer les finances, en temps réel.

La DSI a aussi recours au Help Desk pour fournir une assistance informatique pour tous

les matériels, logiciels et produits de mise en réseau utilisés dans l'entreprise.

Le Help Desk qu'on appelle aussi centre d'assistance informatique ou centre de support informatique, est un service d'assistance interne ou externe qui peut se présenter sous forme de groupe ou de fonction organisationnelle, qu'un utilisateur de l'informatique appelle pour obtenir de l'aide pour résoudre un problème.

Il peut être composé d'une seule une personne qui prend les appels. Comme il peut s'agir d'une organisation mondiale qui accepte les demandes d'assistance soumises en ligne ou en personne depuis le monde entier.

La fonction de service d'assistance est souvent sous-traitée à des spécialistes de l'assistance qui fournissent de l'aide aux utilisateurs d'une entreprise.

2.1. La cellule sécurité des systèmes d'information

L'évaluation des risques opérationnels SI est la mission principale de la CSSI, et la raison pour laquelle elle a été créée. Cette mission est du domaine du responsable SSI, elle s'effectue grâce à des missions d'audit informatique qui ont pour objectif d'identifier, d'évaluer et de déterminer les risques (opérationnels, financiers, de réputation…) associés aux activités informatiques.

L'audit informatique, aussi appelé « audit des systèmes d'information ou de l'anglais Information Technology Audit » consiste à une intervention réalisée par une personne indépendante et extérieure au service audité, qui permet d'analyser tout ou une partie d'une organisation informatique, d'établir un constat des points forts et des points faibles et dégager ainsi les recommandations d'amélioration. Autrement dit, L'audit informatique peut aussi être défini l'évaluation des risques des activités informatiques, dans le but d'apporter une diminution de ceux-ci et d'améliorer la maîtrise des systèmes d'information. (Yende, 2018, p.9)

L'audit informatique se divise en six sous audit qui sont (Yende, 2018) :

- **Audit de la fonction informatique :** qui répond aux questionnements de la DG/DSI sur l'organisation de la fonction informatique, son pilotage, son positionnement dans la structure, ses relations avec les utilisateurs, ses méthodes de travail ;

- **Audit des études informatiques** : cet audit s'assure de l'efficacité de l'organisation, de la structure et du pilotage du SI, la maîtrise de ses activités… ;

- **Audit de l'exploitation :** qui a pour but de s'assurer que les différents centres de production informatiques fonctionnent de manière efficace et qu'ils sont correctement gérés ;

- **Audit des projets informatiques :** il assure le bon déroulement des opérations pour à la fin avoir une application qui sera performante et opérationnelle ;

- **Audit d'une application opérationnelle** : son but est de donner au management une assurance raisonnable sur le fonctionnement d'une application ;

- **Audit de la sécurité informatique :** qui a pour but de donner au management une assurance raisonnable du niveau de risque de l'entreprise lié à des défauts de sécurité informatique. Surtout que maintenant avec le développement de la technologie et d'internet, les risques sont en constantes évolution, et deviennent de plus en plus dangereux.

  La CSSI fait souvent (au moins 1 fois par an) des audits de sécurité informatique pour vérifier le niveau de sécurité de son système SWIFT, et cela en prenant en considération l'affaire de la banque centrale du Bengladesh qui a connu, durant ces dix dernières années, des cyberattaques sur son système SWIFT, ce qui a induit des pertes importantes (81 M€) (La finance pour tous, 2022).

Créée en 1973, SWIFT est une coopérative internationale détenue par ses membres et le premier fournisseur mondial de services de messagerie financière sécurisés.

SWIFT n'effectue pas des transferts de fonds et ne gère pas les comptes des clients, mais centralise les ordres de virement entre les clients de différentes banques et leurs permet de communiquer en toute sécurité, d'échanger des messages financiers standardisés en toute fiabilité, facilitant ainsi les flux financiers internationaux et locaux, et appuyant les échanges et le commerce dans le monde entier. (Le site de SWIFT, https://www.swift.com/)

Depuis les tentatives de Phishing qu'elle a subies, et compte tenu de sa place centrale dans le système financier international. SWIFT a dû renforcer la sécurité des échanges en généralisant en 2021 l'utilisation de l'authentification à double facteur pour les messages concernant des transferts de fonds entre banques. Comme par exemple les clés physiques USB tel que celle Yubico, qui garantit le meilleur niveau de sécurité.

Ce qui n'a pas empêché la BNA, par l'intermédiaire de son RSSI de toujours effectuer des testes d'intrusions techniques et mettre à épreuve la sécurité de son SI.

2.1.1. Teste d'intrusions techniques

Également connu sous le nom de test de pénétration, en anglais « Pen-testing » est une forme de piratage éthique « Ethical Hack », réalisé par les testeurs qu'on appelle « White Hat ». Ces testeurs d'intrusions utilisent des stratégies et des outils conçus pour accéder à des systèmes informatiques, afin de simuler une cyberattaque dans le but d'évaluer l'efficacité des mesures de sécurité de l'information au sein de l'organisation.

Les professionnels de la sécurité utilisent aussi le Pen-testing pour vérifier la conformité réglementaire de leur SI, et pour la sensibilisation de ses employés à la sécurité et la capacité de l'organisation à identifier et à répondre aux problèmes et incidents de sécurité, tels que les accès non autorisés. (Imperva, 2021)

En fonction des objectifs de l'organisation, voici quelques stratégies de tests de pénétration couramment utilisées (contrast Security, s. d.)

- Les tests externes à l'organisation à l'aide de procédures réalisées depuis l'extérieur des systèmes de l'organisation, et les tests internes à l'environnement de l'organisation ;

- Les tests à l'aveugle : son but est de tenter de simuler les actions d'un véritable pirate informatique en disposant que des informations publiques de l'organisation. Et les tests en double aveugle ou seule quelques personnes au sein de l'organisation sont mises au courant.

- Les tests ciblés qui impliquent à la fois les équipes informatiques et les équipes de tests d'intrusion, qui sont au courent dès le départ de la cible et la conception du réseau.

Il existe plusieurs outils permettant de réaliser le piratage éthique et les tests de pénétration. Linux est l'un des systèmes d'exploitation qui offre toute une panoplie de logiciels et de distribution qui contiennent divers outils tout préparés et dédiés à cet effet.

La distribution la plus utilisé pour le Hacking et le Pen-testing est Kali Linux. Doté d'une utilisation facile, certain de ces outils permettent de lancer facilement un scan d'un serveur ou d'une page web sans pour autant être un hacker professionnel.

Parmi les outils de Kali Linux on a Nmap qui est le plus populaire pour la collecte d'informations (adresse IP, le nombre de ports ouverts…).

On a aussi Lynis qui est un outil puissant pour l'audit de sécurité, les tests de conformité et le renforcement des systèmes. On peut aussi citer WordPress, Aircracking, Hydra et pleins d'autres. (Ankush Das, 2020)

Le RSSI s'occupe aussi de dresser les indicateurs de sécurité SI qu'ils appellent « la triade ». On a l'intégrité, la disponibilité, et la confidentialité. Ces indicateurs ne sont pas encore chiffrés en raison de l'absence du tableau de bord de sécurité SI. Ceci est un projet en cours qui est introduit dans le plan d'action de la CSSI.

2.2. Les missions de la cellule sécurité des systèmes d'information

Ajouté à ce qui a été coté auparavant, la circulaire propose à la CSSI énonce les missions suivantes :

- La mise en place et la mise à jour régulière du système de management de la sécurité su SI de la banque en accord avec les objectifs de la DG ;
- L'évaluation et la mise en place du plan de continuité de l'activité informatique en collaboration avec les opérationnels, ainsi que des plans de secours et de sauvegarde informatique ;
- L'évaluation et la mise en place d'un processus de gestion des incidents de sécurité SI, ainsi que des procédures et des normes techniques relatives à la sécurité informatique ;
- Le contrôle permanent du respect des habilitations informatiques et de l'intégration de la sécurité informatique dans les projets ;
- Assurer la veille technologique et le suivi des évolution réglementaires relatives à

la sécurité SI, ainsi que leurs bonnes applications ;

- La coordination des investigations avec la DGR en cas d'incidents de sécurité opérationnel, et avec la DCP en cas d'incidents majeurs ;
- Réaliser les actions de formation et de sensibilisation en vue de promouvoir et de maintenir une culture de sécurité SI auprès de l'ensemble des collaborateurs ;
- Représenter la banque auprès des organismes externes pour des questions relevant de son domaine d'activité.

2.3. Compétences des auditeurs en matière de SI

Pour pouvoir réaliser un audit informatique certaines conditions doivent être remplie. L'audit informatique est une mission qui exige des auditeurs certifiés en l'évaluation des SI, et doivent avoir de fortes connaissances en informatique. (Yende, 2018)

La BNA est en train d'inscrire ses auditeurs à obtenir la certification et les compétences requise pour ce genre de mission. Pour l'instant tout ce qui concerne les missions l'évaluation de la sécurité SI vis-à-vis des risques sont externalisés et réalisés par des prestataires étrangers à l'organisation.

Il existe deux grandes certifications de référence mise au point par ISACA (Information System Audit and Control Association) :

- **La certification CISA (Certified Information System Auditor)** qui permet de bénéficier d'un module de la certification CIA de l'Institute of Internal Auditors (IIA), dont l'examen se passe trois fois par an, dans 11 langues différentes et dans 200 villes dans le monde. Il faut répondre de 150 à 200 questions à choix multiples en 4 heures portant sur l'audit et l'informatique. L'examen porte sur six domaines :

    - Les processus d'audit des systèmes d'information ;
    - La, gouvernance IT ;
    - La gestion du cycle de vie des systèmes et de l'infrastructure ;
    - La fourniture et le support des services ;
    - La protection des avoirs informatiques ;
    - Le plan de continuité et le plan de secours informatique.

- **La certification CISM (Certified Information Security Manager),** pour les managers en sécurité de l'information délivrée également par l'ISACA. Cette certification est subdivisée en deux grandes catégories : CRISC (Certified in Risk and Information System Control) et CGEIT (Certified in the Governance of Entreprise IT). Le programme de la certification CISM est composé de cinq domaines de la sécurité de l'information :

    - La gouvernance de la sécurité de l'information ;
    - La gestion des risques de l'information ;
    - L'implémentation d'un programme de sécurité de l'information ;
    - La gestion d'un programme de sécurité de l'information ;
    - La gestion des incidents de sécurité de l'information.

2.4. Référentiel normatif pour la gestion des risques SI de la BNA

Avant la DRCP utilisait COSO et CobiT pour la cartographie des processus et des différents risques que subit la BNA. Mais maintenant qu'une cellule spécialisée dans la sécurité SI a été créée CSSI. Cette dernière est en train d'œuvrer pour obtenir une certification ISO 27005 « Technologies de l'information. Techniques de sécurité. Gestion des risques liés à la sécurité de l'information ». Cette norme contient des lignes directrices relatives à la gestion des risques en sécurité de l'information dans un organisme.

ISO 27005 est conçu pour aider à la mise en place de la sécurité de l'information basée sur une approche de gestion des risques. Elle est à tous types d'organismes qui ont l'intention de gérer des risques susceptibles de compromettre la sécurité des informations de l'organisme.

Avant de suivre et d'appliquer les directives de l'ISO 27005, il est important de connaître les concepts, les modèles, les processus et les terminologies décrites dans l'ISO/IEC 27001 et l'ISO/IEC 27002.

La DRCP est aussi en train d'étudier et d'ouvrer pour obtenir une certification ISO 31000 « Risk Management ».

Pour ce qui est des méthodes de gestion des risques SI, la CSSI a opté pour la méthode

EBIOSE (mentionné dans le chapitre 1, section 3, point 1.3), après avoir essayé la méthode MEHARI.

2.5. Les risques opérationnels liés au SI de la BNA

Parmi les innombrables risques opérationnels qu'un SI peut rencontrer, les risques de cybersécurités sont les plus courants au sein de la BNA, et plus particulièrement les tentatives de phishing. Ce risque n'est pas classé parmi les risques majeurs étant donné que la BNA est à cheval sur la sécurité de l'information.

La plupart du temps le SI de la BNA fait face aux risques physiques tel que les coupures de courant dans l'une des agences, ou bien un site qui se plate quand celui-ci ne respecte pas les normes.

Ces risques heureusement, n'ont jamais eu d'impacts financier sur l'établissement. Ils touchent beaucoup plus l'image de l'organisation quand par exemple un client est mécontent quand l'une des agences est en hors service.

3. Le processus de management des risques de la BNA

Pour l'instant la B.N.A n'a pas mis en place de processus de management des risques, ce dernier étant un projet en cours d'exécution, elle fait face aux risques en dressant des plants d'action par la DGR, des plants stratégiques ainsi que des plans de continuité d'activité et de sécurité des systèmes d'information. Les données étant confidentiels, il nous est impossible de détailler plus ces points.

Conclusion

Dans le cadre de ce dernier chapitre, nous avons traité à travers des entretiens et des questionnaires, les pratiques de la gestion des risques opérationnels liés au système d'information de la BNA, et le rôle que joue la direction d'audit dans le processus ERM.

Notre étude nous a permis de connaître les procédures qu'entreprend la BNA pour parer aux risques de son système d'information. Connaitre l'existence ou non d'un processus ERM, et l'éventuel rôle que peut jouer la fonction d'audit interne dans ce dernier.

Pour cela, nous avons décrit les différents éléments que constitue l'organisation général de la BNA, et nous avons découvert que cette banque a toute une division consacrée à la gestion des risques et du contrôle permanent DRCP. Parmi ses composantes, nous avons découvert l'existence d'une cellule expressément dédier à la sécurité SI.

Ensuite, nous avons présenté la contribution de la fonction d'audit dans le management des risques, notamment en ce qui concerne l'élaboration de la cartographie des risques.

A l'issue de ce travail, nous avons constaté que l'environnement de la BNA en ce qui concerne la gestion des risques est évolutif. L'absence temporaire d'un processus ERM correspondant aux normes récentes, ne l'a pas empêché d'avoir des dispositifs très pointues pour la gestion des risques SI, et d'œuvrer pour l'améliorer et migrer vers de nouvelles procédures encore plus performantes.

La fonction d'audit de la BNA, est toujours présente en ce qui concerne l'amélioration du contrôle interne et au management des risques. La DAI est impliquée dans tous les processus, et elle aide la BNA à réaliser ses objectifs dans un contexte de plus en plus exigent où la performance doit être placée au cœur des interventions.

Conclusion générale

Dans le but de répondre à notre problématique qui s'articule autour du rôle que peut jouer l'audit interne dans l'amélioration du processus de management des risques opérationnels lié aux systèmes d'information, nous avons choisis de diviser notre travail en deux paries intiment liés.

La première partie qui représenta le cadre théorique de notre mémoire est subdivisé en deux chapitres. Le premier qui porte le titre de « gestion des risques opérationnels des systèmes d'informations », nous a permis de comprendre que l'organisation moderne est confrontée à une multitude de risques qui peuvent affecter son efficacité opérationnelle et sa conformité réglementaire.

Ajouté à cela, le recourt aux technologies de l'information comme moyen de contenir et de gérer l'information qui est le noyau de chaque organisation, génère une multitude de risques opérationnels comme la cybersécurité, et la simple prise de conscience ne suffit pas pour en venir à bout. Ce qui pousse les organisations à chercher des moyens efficaces pour gérer et contenir ces risques.

C'est là que la gestion des risques entre en jeu. Cette fonction aide les organismes à gérer, à minimiser et, dans certains cas, à éliminer les risques informatiques, y compris en matière de sécurité de l'information, afin de préserver la sécurité et l'activité.

Le second chapitre nommée « Entreprise Risk management et la fonction d'audit », nous a permis de comprendre que pour suivre l'augmentation de la fréquence de défaillances et d'appariation des risques, il est nécessaire de disposer d'outils de maitrise des risques de plus en plus efficaces, accompagné d'une véritable culture de management et contrôle des risques diffusés aussi bien dans les fonctions administratives que dans les fonctions opérationnelles des organisations.

Le management des risques d'entreprise est un processus qui permet de planifier, d'organiser, de diriger et de contrôler les activités d'une organisation afin de réduire les coûts opérationnels et améliorer les revenus. Ce processus ERM comprend tous les types de risques, et il est compatibles avec chaque organisation peu importe son activité.

Un intérêt accru est porté sur l'ERM notamment par les organismes de réglementation

de l'industrie et des gouvernements, ainsi que les investisseurs, qui examinent de plus près les politiques et procédures de gestion des risques des entreprises. De ce fait, les conseils d'administration sont tenus d'examiner et de rendre compte de l'adéquation des processus de gestion des risques dans leurs organisations.

A la fin de notre théorie, nous avons pu découvrir que le management des risques et l'audit interne sont intimement liés. Ce dernier peut fournir des services de conseil qui améliorent la gouvernance, et plus spécialement, les processus de contrôle et de management des risques.

Le rôle de l'audit interne est de fournir une assurance sur l'efficacité du processus utilisé pour le management des risques d'entreprise, à condition que cette activité ne compromette pas l'indépendance et l'objectivité de l'audit interne.

L'audit interne, a de nombreuses possibilités d'élargir son champ d'action traditionnel et d'apporter une valeur ajoutée à son organisation en matière de management des risques. Ce champ dépendra des autres ressources, internes et externes, dont dispose le conseil d'administration et de la maturité de l'organisation en matière de risques. Sans pour autant dépasser certaines limites énoncées par l'IIA.

Selon le même organisme, l'audit interne se doit d'évaluer le processus de management des risques et contribuer à son amélioration. Cette évaluation peut se faire à travers plusieurs méthodes et approches que nous avons cité, à savoir, l'approche par éléments du processus, l'approches par principe clés, et enfin l'approche par model de maturité comme le CMMI.

Pour compléter notre travail, nous avons réalisé une enquête au niveau de la Banque Nationale d'Algérie « B.N.A ». Au travers de ce dernier chapitre, nous avons essayé, malgré les contraintes de confidentialité et d'absence d'informations, de présenter du mieux que possible la structure de la B.N.A, tout en se basant sur la division risques et contrôle permanent et surtout, sur la direction d'audit interne.

Notre étude nous a permis de souligner et d'expliquer si la direction d'audit interne de la B.N.A participait, effectivement, au processus de management des risques. Ainsi, nous avons, tout d'abord, chercher à décrire le processus ERM de la B.N.A, ainsi que ses

acteurs.

Ce qui nous a permis à découvrir que cette dernière, malgré son rôle stratégique et sa position économique et financière en Algérie et à l'étranger, ne possède qu'un dispositif de management des risques, et que l'ERM est qu'un projet en cours de réalisation.

Ensuite, nous avons présenté la contribution de la DAI à ce dispositif. Cette participation s'explique par l'évaluation des procédures organisationnelles, de pilotage et de contrôle des structures centrales de la B.N.A et l'élaboration de la cartographie des risques.

La direction d'audit interne de la B.N.A, participe à l'amélioration du contrôle interne et au management des risques. Ce qui permet à cette banque de réaliser ses objectifs dans un contexte de plus en plus exigent où la performance doit être placée au cœur des interventions.

En ce qui concerne la sécurité informatique, la B.N.A est grandement consciente que les risques en matière de sécurité de l'information doivent être couverts. Pour cela elle n'a pas hésité à créer une cellule dédiée à la sécurité des systèmes d'information. Cette dernière s'occupe de mettre en place des plans d'audit traités par des auditeurs spécifiquement formés, suivis par des plans d'actions qui donnent lieu à l'émission de recommandations validés et suivis par la direction générale.

Bien que la notion d'ERM a été introduite en 2004, sa mise en œuvre n'est pas encore largement utilisée et se développe. Depuis, de nombreuses organisations sont encore en train d'élaborer leur propre procédure de gestion des risques.

De nombreux arguments et débats subsistent sur l'implication et le rôle de l'audit interne dans la gestion des risques. Mais si l'ERM est absent dans une organisation, comme c'est le cas momentanément chez la B.N.A. l'IIA, à travers son guide sur les processus de management des risques, précise clairement que l'audit interne ici joue un rôle important dans l'optique de promouvoir la démarche ERM, en essayant de convaincre la direction générale de construire un véritable processus de management des risques, car cela va permettre à l'organisation d'être réactive face aux risques dans un environnement technologique imprévisible.

L'audit interne peut aussi participer, ou bien à lui seul, identifier, évaluer et réaliser une

première cartographie des risques de l'organisme, en adoptant une approche processus. Il peut même être amener à gérer ce processus, et à coordonner les actions de ses divers acteurs après sa création. L'audit interne ne doit pas cependant oublier qu'il n'en est pas pour autant le propriétaire.

En conclusion, la réalité de l'environnement commercial actuel, en constante évolution, a fait du management des risques d'entreprise, un élément fondamental de la gouvernance d'entreprise. Les organisations jettent un regard neuf sur la manière dont elles géraient les risques, et elles ont compris l'importance d'un processus ERM efficace.

La réussite de la mise en œuvre d'un processus ERM, dépend grandement de la stratégie de l'organisation, qui doit comporter une compréhension approfondie de toutes les hypothèses qui l'accompagnent. Notamment, en forment correctement leurs employés au management des risques, et en impliquant la fonction d'audit interne, de par ses compétences, à l'établissement et à la mise en œuvre en œuvre du processus de management des risques d'entreprise ERM.

Ceci permettra aux organisations de mieux faire face à l'évolution du climat économique et créer un environnement de travail plus conscient. Ce qui contribuera à les protéger contre toute turbulence qu'elles peuvent confrontées à l'avenir.

Bibliographie

Livres :

~ Gillet M. et Gillet P. (2010). Système d'information des ressources humaines (1ère édition). Paris : Dunod

~ Rosnay J. D. (1975). Le macroscope. Vers une vision globale (1ère édition). Paris : Seuil

~ Tawfik L. et Chauvel A. M. (1980). Gestion de la production et des opérations. (1ère édition). Paris : HRW Ltée

~ Morley C et all. (2011). Processus métiers et systèmes d'information (3éme édition). Paris : Dunod

~ Reix R. et all. (2016). Système d'information et management (7éme édition). Paris : Vubert

~ Laudon K. et Laudon J. et all. (2013). Management des systèmes d'information (13ème édition). Paris : Pearson

~ Laudon K. et Laudon J. et all. (2010). Management des systèmes d'information (10ème édition). Paris : Pearson

~ Tassin P. (2005). Systèmes d'information et management de crise (1ère édition). Paris : Lavoisier

~ Deyrieux A. (2004). Le système d'information nouvel outil de stratégie (1ère édition). Paris : Maxima

~ Luisot J. P. (2005). Gestion des risques (1ère édition). Paris : AFNOR

~ Schick P. et all (2010). Audit interne et référentiels de risque (1ère édition). Paris : Dunod

~ Darsa J. D. (2013a). La gestion des risques en entreprise (3 -ème édition). France : Gereso

~ Darsa J. D. (2013b). Les risques opérationnels de l'entreprise (1ère édition). France : Gereso

~ Jimenez C. et Merlier P. (2004). Prévention et gestion des risques opérationnels (1ère édition). France : Revue Banque

~ Desroches A. et all. (2005). La gestion des risques (3 -ème édition). Paris : Lavoisier

~ Moisand D. et Garnier De Labareyre F. (2009). Cobit. Pour une meilleure gouvernance des systèmes d'information (1ère édition). Paris : Eyrolles

~ Ségot J. et all. (2011). Management de la qualité et de la performance (1ère édition). France : Lexitis éditions

~ Autorité des Marchés Financiers AMF. (2010). Les dispositifs de gestion des risques et de contrôle interne, cadre de référence. France : IFACI. https://docs.ifaci.com/wpcontent/uploads/2018/03/les_dispositifs_de_gestion_des_risques_et_de_contr%C3%B4le_interne___cadre_de_r%C3%A9f%C3%A9rence___amf__juillet_2010_.pdf

~ Aractingi F. et Canaméras G. (2013). Trois lignes de Maîtrise pour une meilleure performance. France : AMRAE, IFACI. https://docs.ifaci.com/wpcontent/uploads/2018/03/Troislignesdema%C3%AEtrisepourunemeilleureperformance.pdf

~ Institut Français De L'audit Et Du Contrôle Internes. (s. d.). Méthodologie de conduite d'une mission d'audit interne. France : IFACI. https://www.economie.gouv.fr/files/fichesmethodologiques.pdf

~ Groupe Professionnel Industrie et Commerce. (2003). Étude du Processus de Management et de Cartographie des Risques. Guide d'audit, les cahiers de la recherche. Paris : IFACI. https://www.economie.gouv.fr/files/cahier_de_la_recherche_processus_management_et_carto_des_risques.pdf

~ IFACI. (2012). Référentiel professionnel de l'audit interne. Paris : Certification IFACI. https://www.economie.gouv.fr/files/rpai2012-doc_fxc.pdf

~ The Institute of Risk Management, IRM. (2002). A Risk Management Standard. London : IRM https://www.theirm.org/media/4709/arms_2002_irm.pdf

~ Verver J. (2021). 7 étapes à suivre pour bénéficier d'un ERM améliorant vos performances. Galvanize. https://info.wegalvanize.com/7-steps-to-performance-enhancing-ERM-eBook-fr.html

~ Carlier A. (2006). Management de la qualité pour la maîtrise du SI (1ère édition). Paris : Lavoisier

~ Federation Of European Risk Management Associations Ferma. (2003). Cadre de référence de la gestion des risques. AIRMIC, ALARM, IRM : 2002, translation copyright FERMA : Brussels https://www.ferma.eu/app/uploads/2011/11/a-risk-management-standard-french-version.pdf

~ Bursh J.G. et Felix R.S. (1984). Information System Theory and Practice (1st edition). USA: Hamiltow edition.

~ Yatchinovsky A. (2004). L'approche systémique : Pour gérer l'incertitude et la complexité
(1ère édition.). Paris : ESF éd

~ Cordel F. (2013). Gestion des risques et contrôle interne (1ère édition). Paris : Vuibert

~ Dumora R. (2017). Gestion de l'entreprise d'assurance (2ème édition). Paris : Dunod

~ Thevenot J. (2011). Master systèmes d'information (1ère édition). Paris : Eska édition

~ Institut Français Des Administrateurs (2013). Trois lignes de Maîtrise pour une meilleure performance (1ère édition). Paris : AMRAE, IFACI https://docs.ifaci.com/wpcontent/uploads/2018/03/Trois_lignes_de_ma%C3%AEtrise_pour_une_meilleure_performance.pdf

Articles :

~ Mayer N. J. et Humbert P. (Avril-Mai 2006). La gestion des risques pour les systèmes d'information. MISC, (n°24). https://www.nmayer.eu/publis/NMA-JPH_MISC24.pdf

~ Ebondo Wa Mandzila E. et Zéghal D (03 Avril 2009). Management des risques de l'entreprise : Ne prenez pas le risque de ne pas le faire ! La Revue des Sciences de Gestion, (n° 237-238), pages 5 à 14. https://www.cairn.info/revue-des-sciences-de-gestion-2009-3-page-5.htm

~ Sourour H. A. (Janvier 2018). La contribution de l'auditeur interne à l'entreprise Risk Management : résultats d'une étude exploratoire. Recherches en Sciences de Gestion. (n° 127 (4) : 107). https://www.researchgate.net/publication/331251058

~ Yende R. G. (22 Décembre 2018). Support de cours de l'audit des systèmes d'information (INFORMATIQUE). Licence. Audit des systèmes d'information, Congo-Kinshasa. (Cel-01964389) https://hal.archives-ouvertes.fr/cel-01964389/document

~ Ikkou L. et Elouidani A. (Décembre 2016). La gestion des risques des systèmes d'information dans les organismes publics au Maroc : quels bénéfices a la performance ? Revue Économie, Gestion et Société. (n°8). https://revues.imist.ma/index.php/REGS/article/download/7370/4273

~ Weekes-Marshall D. (2020). The role of internal audit in the risk management process : A developing economy perspective. Journal of Corporate Accounting & Finance, ((n° 31(4)).

Pp.154165.https://www.researchgate.net/publication/343982541_The_role_of_internal_auditin_the_risk_management_process_A_developing_economy_perspective

~ Kertali M. et Tahajuddin S. B. (01 Novembre 2018). The Effect of Internal Auditors' Involvement in Enterprise Risk Management on Internal Audit Objectivity: Evidence from Malaysia. Asian Journal of Economics, Business and Accounting, (n°AJEBA.40693). https://www.researchgate.net/publication/324589199

~ El Harchaoui E. (Juillet 2019). La contribution de l'audit interne dans la gouvernance d'entreprise. Finance & Finance Internationale (n° 15).https://revues.imist.ma/index.php /FFI/article/download/17028/9423

~ Maurer F. (2007). Les développements récents de la mesure du risque opérationnel. Revue du financier (n°163). P.34. http://www.ressourcesactuarielles.net/EXT/ISFA/1226.nsf/ 0/fab6e9d2c35626cac1257815003b458b/$FILE/31.pdf

Rapports :

~ Petsetidi Soupe k. et De La Brosse A. (2016). Notre vision du Risk Appétit. Sia Partners. Https://www.eifr.eu/uploads/eventdocs/56f3c65ae750a.pdf

~ World Intellectual Property Organization WIPO (2016). Audit Report. Audit of Enterprise Risk Management. Internal Oversight Division. https://www.wipo.int/aboutwipo/en/over sight/iaod/audit/pdf/enterprise_risk.pdf

~ CBOK Report. (2015). Navigating Technology's Top 10 Risks. IIA Nederland. https: //www.iia.nl/actualiteit/nieuws/cbok-report-navigating-technologys-top-10-risks

Pages internet :

~ Leterme, C. (2020, 14 février). Tout savoir sur la publication d'un article scientifique. Scribbr. Consulté le 02 Mars 2020 Sur : www.scribbr.fr/articlescientifique/publication -article-scientifique

~ Caclin F. (2021). Le risque opérationnel. Fimarkets. Consulté le 13 Octobre 2021 sur https:// www.fimarkets.com/pages/risque_operationnel.php

~ Optimind. (2011, Avril). Risques opérationnels. Quelles réponses face à un risque

difficile à appréhender ? consulté le 23 Octobre 2021 sur https://www.optimind.com/medias/documents/217/avril_dt_risques_operationnels_vf.pdf

~ Institut Des Actuaires. (2016, 08 Novembre). Le risque opérationnel, un nouveau challenge pour l'actuaire. IA. Consulté le 30 Octobre 2021 sur https://www.institutdesactuaires.com/global/gene/link.php?docid=9761&fg=1

~ Dale F Cooper. (2007). Tutorial Notes: The Australian and New Zealand Standard on Risk Management, AS/NZS 4360 :2004. Broadleaf Capital International Pty Ltd. Consulté le 13 Février 2022 sur http://broadleaf.com.au/old/pdfs/trng_tuts/tut.standard.pdf

~ Sallou E. (2019). Evaluer les processus de management des risques. Consulté le 16 Mars 2022 sur https://apprendrelaudit.com/evaluer-les-processus-de-management-des-risques/

~ IONOS (2020). Une gestion des risques normalisée : ISO 31000. Consulté le 25 Avril 2022 sur https://www.ionos.fr/startupguide/gestion/iso-31000/

~ Certification QSE, s. d). Approche processus et Management par approche Système. Consulté le 25 Avril 2022 sur https://www.certification-qse.com/approche-processus/

~ Takyorian J. F. (2003). Maturité des processus et amélioration continue. Consulté le 26 Avril 2022 sur https://www.infoqualite.fr/maturite-des-processus-et-ameliorationcontinue/

~ L'Equipe de La finance pour tous. (15 Mars 2022). Qu'est-ce que SWIFT ? consulté le 05 Juin 2022 sur https://www.lafinancepourtous.com/outils/questions-reponses/quest-ce-que-swift/

~ Contrast security (s. d.). What is penetration testing? Consulté le 05 Juin 2022 sur https://www.contrastsecurity.com/glossary/penetration-testing

~ Ankush Das A. (2017). 21 Best Kali Linux Tools for Hacking and Penetration Testing. Consulté le 08 Juin 2022 sur https://itsfoss.com/best-kali-linux-tools/

Conferences:

~ Kigen K. (28 Octobre 2019). Internal Audits Role in Enterprise Risk Management. [Conference]. 2019 Super Conference Presentations. University of North Texas https://www.dallasiia.org/wp-content/uploads/2019/10/Internal-Audits-Role-inEnterprise-

Risk-Management.pdf

Normes et référentiels normatifs :

~ IFACI. (2017). Le management des risques de l'entreprise, Cadre de Référence. Synthèse. COSO et PwC. https://www.ifaci.com/wp-content/uploads/COSO-ERM2017_synthe%
CC%80se.pdf

~ Guide 73, 2009. Management du risque — Vocabulaire https://www.iso.org/obp/ui/#iso:std
:iso:guide:73:ed-1:v1:fr

~ IIA. (2009). IIA position paper: the role of internal auditing in enterprise-wide risk management. p. 4. https://www.theiia.org/en/content/position-papers/2009/the-roleof
internalauditing-in-enterprise-wide-risk-management/

~ IFACI. (2002). Normes professionnelles de l'audit interne. Paris : IFACI

~ IFACI. (2017). Le management des risques de l'entreprise Une démarche intégrée à la stratégie et à la performance, synthèse. (Initialement publié par COSO en 2017). https://www.ifaci.com/wp-content/uploads/COSO-ERM-2017_synthe%CC%80se.pdf

~ IIA. (2004). Applying COSO's Enterprise Risk Management — Integrated Framework. https://www.consiglionazionaleforense.it/documents/25901/232833/Enterprise+Risk+Management.pdf/313be550-3871-4927-9dbf-480fe823f768?t=1471875232000

~ IIA. (2020). Le modèle des trois lignes de l'IIA. https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-anupdate-of-the-three-lines-of-defense-ju
ly-2020/three-lines-model-updated-french.pdf

~ International Organization for Standardization/ Technical Committee. (2018). Management du risque — Lignes *directrices* (ISO Standard No. 31000 :2018).
~ International Organization for Standardization/ International Electrotechnical Commission. (2000). Ingénierie des systèmes et du logiciel — Exigences de qualité des systèmes et du logiciel et évaluation (ISO Standard No. 9000 :2000).
~ International Organization for Standardization/ International Electrotechnical Commission. (2015). Système de mangement de la qualité — principes essentiels et vocabulaire (ISO Standard No. 9000 :2015).
~ International Organization for Standardization/ International Electrotechnical

Commission. (2018). Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information (ISO Standard No. 27005 :2018).

Dictionnaires :

~ Larousse. (S. d.). Entreprise. Dans Le Dictionnaire Larousse en ligne. Consulté le 06 janvier 2022 sur https://www.larousse.fr/dictionnaires/francais/entreprise/30069

~ Larousse. (s. d.). Informatique. Dans Le Dictionnaire Larousse en ligne. Consulté le 17 Mars 2022 sur https://www.larousse.fr/dictionnaires/francais/informatique/42996

~ Larousse. (s. d.). Risque. Dans Le Dictionnaire Larousse en ligne. Consulté le 04 Novembre 2021 sur https://www.larousse.fr/dictionnaires/francais/risque/69557

Thèses :

~ Raïs H. M. (2012). Gestion des risques : Mesures et Stratégies. [Thèse de doctorat, Université Toulouse 1 Capitole (UT1 Capitole)]. http://www.theses.fr/2012TOU10063.pdf

~ Mashal R. (2012). Internal Audit Roles in Risk Management from Risk Management Perspective : New Vision. [Jordan Risk Management Center for Training, (JRMC)]. https://www.researchgate.net/publication/237150266_Internal_Audit_Roles_in_Risk_Management_from_Risk_Management_Perspective_New_Vision

~ Ferchichi A. (2008). Contribution à l'intégration des processus métiers : application à la mise en place d'un référentiel qualité multi-vues. [Thèse de doctorat, Ecole Centrale de Lille ; Ecole Centrale Paris)]. https://tel.archives-ouvertes.fr/tel-00295306

~ Mazouni M. H. (2008). Pour une meilleure approche de management des risques : de la modélisation ontologique du processus accidentel au système interactif d'aide à la décision. [Thèse de doctorat, Institut National Polytechnique de Lorraine (INPL)]. https://tel.archives-ouvertes.fr/tel-00338938v1

Liste des tableaux et des figures

Liste des tableaux

Liste des figures

Annexes

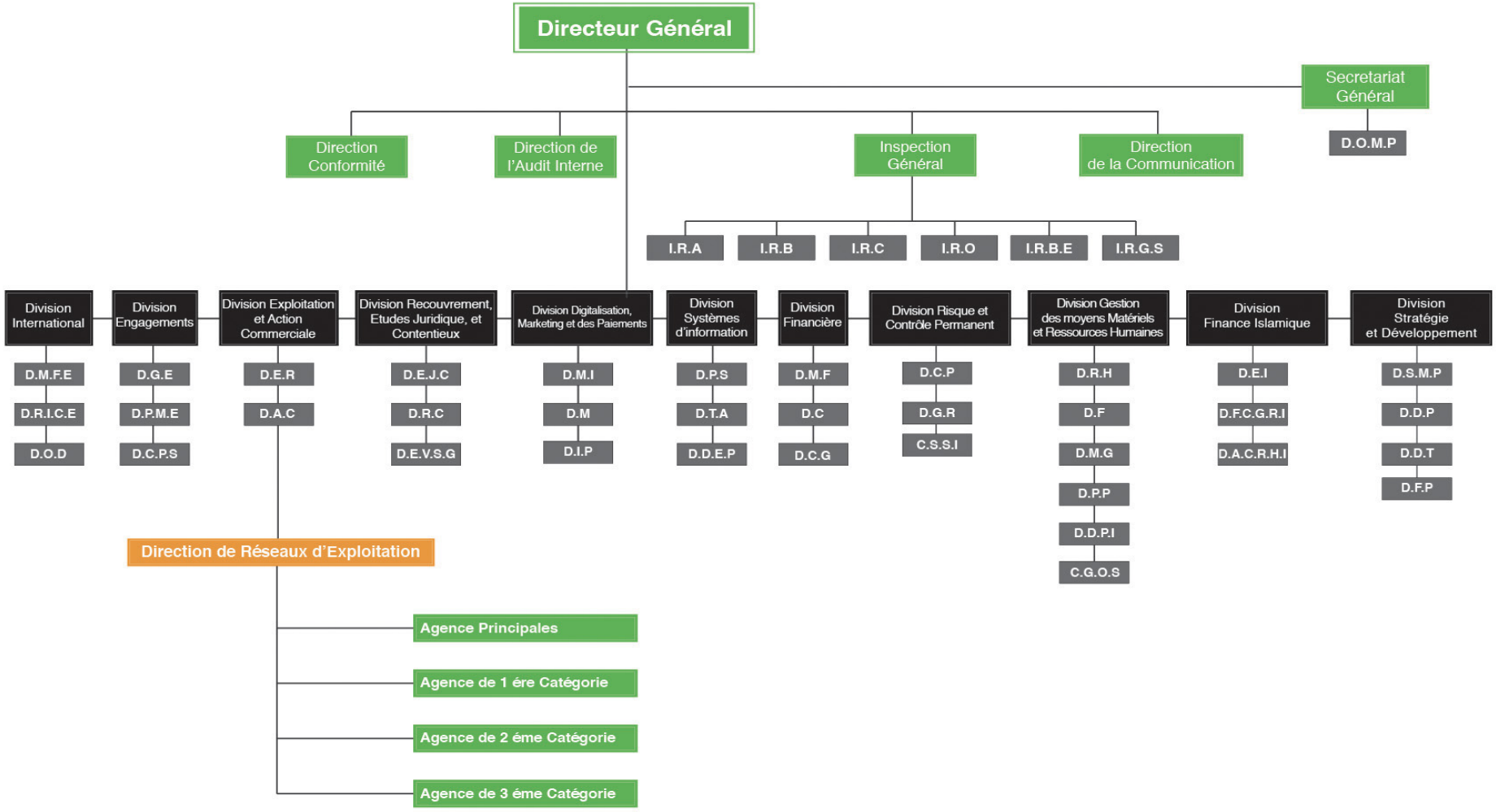
Annexe 01 : Organigramme de la B.N.A

Annexe02 : Extrait du règlement n°2011-08 du 28 novembre 2011 relatif au contrôle interne des banques et établissements financiers

Annexe 03 : Extrait du règlement n°2014-02 du 16 février 2014 relatif aux grands risques et aux participations

Annexe 04 : Questionnaire

Annexe 01 : organigramme de la BNA.



Annexe 02 : Extrait du règlement n°2011-08 du 28 novembre 2011 relatif au contrôle interne des banques et établissements financiers

Article 27 : Les banques et établissements financiers mettent en place des procédures de centralisation et d'évaluation des informations relatives aux éventuels dysfonctionnements dans la mise en œuvre effective des obligations de conformité. Ils s'assurent régulièrement du suivi des actions correctrices engagées.

Les procédures, visées ci-dessus, prévoient en particulier la faculté pour tout dirigeant ou préposé de faire part au responsable du contrôle de la conformité, ou à un de ses délégués, d'interrogations sur d'éventuels dysfonctionnements relatifs à la conformité, notamment à propos de la régularité d'opérations ou de la conformité d'agissements au regard des dispositions relatives aux conflits d'intérêts ou à la déontologie professionnelle. Cette faculté et ses modalités de mise en œuvre sont portées à la connaissance de tous les agents.

Annexe 03 : Extrait du règlement n°2014-02 du 16 février 2014 relatif aux grands risques et aux participations

Article 15 : Les banques et établissements financiers doivent disposer d'un rapport d'audit externe sur les risques qu'ils encourent sur toute entreprise constituant un grand risque, au sens de l'article 2 du présent règlement.

Article 16 : Les banques et établissements financiers élaborent périodiquement des scénarios de crise portant sur la dégradation des risques de crédit des principales contreparties.

Ces scénarios doivent notamment tenir compte des concentrations du risque de crédit et de la valeur de réalisation des garanties y attachées.

Article 17 : Les banques et établissements financiers doivent déclarer trimestriellement leurs grands risques suivant les dispositions arrêtées par une instruction de la Banque d'Algérie.

Annexe 04 : Questionnaire

I - Cadre organisationnel de la gestion des risques SI.			
Question	**Réponse**		**Observations**
1- La notion du risque est-elle présente dans votre établissement ?	Culture du risque		
	Typologies		
	Définition du risque opérationnel		
	Fonction de gestion des risques opérationnels		
	Responsable des risques (risque manager)		
2- Votre établissement a-t-il défini ses objectifs en matière de gestion des risques ?	Oui	Non	
3- Parmi les objectifs managériaux de votre organisation, la question de la sécurité de votre système d'information est-elle abordée ?	Oui	Non	

4- A-t-on mis en place des procédures pour identifier les principaux risques pouvant affecter votre système d'informations ?	Oui	Non	
5-Existe-t-il un responsable de la sécurité des SI ?	Oui	Non	
6- Les responsabilités en matière de gestion des risques sont-elles définies et communiquées aux personnes concernées ?	Oui	Non	
7- Le responsable de la gestion des risques dispose-t-il des qualifications suffisantes pour exercer son autorité auprès des opérationnels et des dirigeants ?	Oui	Non	
8- Une politique et des procédures de gestion des principaux risques ont-elles été définies, validées par la Direction et mises en place dans la société ?	Oui	Non	

9- La société a-t-elle identifié les obligations légales et réglementaires applicables en matière de communication sur les risques ?	Oui	Non		
10- La DSI évalue-t-elle régulièrement les risques SI ?	Oui	Non		
11- La DSI a-t-elle définit des indicateurs clés de performance de votre SI ?	Oui	Non		
12- Quel référentiel utilisez-vous pour la gestion des risques SI ?	Cobit			
	Coso			
	ISO 31 000			
	Autre			
	EBIOS			
13- Quelle méthode suivez-vous pour la gestion des risques de votre système d'information ?				
	OCTAVE			
	MEHARI			
	Autre			
14 - Avez-vous, par le passé, fait face à l'un de ces risques opérationnels ?	Oui	Non		

	Cybersécurité		
	Protection des données		
	Projets SI		
	Gouvernance des SI		
	Prestations informatiques externalisées		
	Utilisation des réseaux sociaux		
	Informatique mobile		
	Compétences des auditeurs internes en matière de SI		
	Technologies émergentes		
	Sensibilisation du conseil et du comité d'audit		
15- Quel était l'impact de ces risques sur les objectifs de votre établissement ?			

II. Prise de connaissance du processus de management des risques de l'organisation.

1- Existe-t-il un processus de management des risques menaçants les objectifs de votre organisation ? Si oui de quelle référence provient-il ?	Oui	Non	
	COSO		
	ISO 31 000		
2- Existe-t-il des responsables/acteurs impliqués dans l'élaboration de votre ERM ? Si oui, qui sont-t-ils ?	Oui	Non	
	La direction générale		
	Le comité d'audit		
	Le conseil d'administration		
	Comité des risques		
	Responsable des risques		
	Comité exécutif de management des risques		
	Les différents responsables de direction, de divisions, de service		
	Autres		
3- La cartographie des risques se fait-t-elle à partir de l'ERM ?	Oui	Non	
4- L'ERM évalue-t-il les risques en fonction des trois critères ci-dessus ?	Impact		
	Probabilité d'occurrence		
	Niveau de maitrise de contrôle		

5. Le control interne et l'ERM fonctionnent-t-ils de manière coordonnée pour réaliser les activités suivantes ?	Cartographie et évaluation des risques			
	Définition et évaluation des activités de contrôle			
	Pilotage et diffusion de l'information			
	Supervision continue			
6- Des seuils de niveau d'acceptabilité des risques ont-ils été définis par le management ?	Oui	Non		
7- Pour chacun des risques identifiés, a-t-on mis en place l'une des mesures de traitement suivantes :	Acceptation			
	Reduction			
	Elimination			
	Assurance/transfère			
8- Existe-t-il un plan d'action sur les risques qui nécessitent d'être réduits ?	Oui	Non		
9- L'ERM subit-t-il des évaluations par l'audit interne ? Quelle approche utilisez-vous	Oui	Non		
	Approche par principe clés			
	Approche par élément du processus			

	Approche par modèle de maturité		
10- Votre processus ERM couvre-t-il les caractéristiques suivants ?	Pilotée par les données Bâtie sur les faits réels		
	Dynamique Réactive face aux risques en constante évolution et aux événements connexes.		
	En continu Fournit des informations constantes et opportunes en temps réel.		
	Exhaustive Prend en compte tous les aspects de toutes les formes de risques		
	Collaborative S'assure que les trois lignes de défense fonctionnent de manière harmonisée autour de leurs responsabilités respectives.		
	Tournée vers l'avenir Fournit des notifications de ce qui se passe, de ce qui est susceptible de se produire et de ce qui doit être fait en conséquence.		
	Contextuelle Fournit des informations pertinentes pour les responsables à différents niveaux et fonctions, et s'aligne sur les objectifs généraux de l'entreprise.		
	Hautement efficace Pilotée par une technologie conçue spécifiquement pour effectuer tout ce qui précède		

11- Avez-vous obtenu une certification de conformité de votre ERM aux normes du CRIPP ?	Oui	Non		
12- L'évaluation de votre ERM a-t-elle permis de couvrir les objectifs suivants ?	Les objectifs stratégiques et opérationnels de l'organisation sont cohérents avec sa mission et y contribuent.			
	Les risques significatifs sont identifiés et évalués.			
	Les modalités de traitement des risques retenues sont appropriées et en adéquation avec l'appétence pour le risque de l'organisation.			
	Les informations relatives aux risques sont recensées et communiquées en temps opportun au sein de l'organisation pour permettre au personnel, aux membres du management et au conseil d'exercer leurs responsabilités.			

Table des matières

Résumé :

Les organisations sont aujourd'hui confrontées à une multitude de risques qui peuvent affecter leurs pérennités et leurs croissances, notamment les risques informatiques compte tenu de l'omniprésence des technologies de l'information dans leurs activités, à mesure qu'elles se digitalisent.

La gestion des risques informatiques est le processus continu d'identification, d'analyse, d'évaluation et de traitement des expositions aux risques, dont ceux liés systèmes d'information, pour atténuer leurs effets négatifs.

Enterprise Risk Management « ERM » est un processus méthodologique qui élargit le domaine de la gestion des risques au niveau stratégique de l'organisation, pour se prémunir contre les risques et autres dommages potentiels qui peuvent interférer avec les opérations et les objectifs de celle-ci.

Le processus ERM et la fonction d'audit interne sont intimement liés, cette dernière a pour rôle de fournir une assurance objective au conseil d'administration sur l'efficacité des activités de l'ERM. Pour comprendre cette liaison, nous avons essayé d'étudier de quel façon l'audit interne procède-il à l'amélioration du processus de management des risques SI.

Mots clés : systèmes d'information, risques opérationnels, management des risques, processus ERM, audit interne, performance.

Summary:

Organizations today face a multitude of risks that can affect their sustainability and growth, including IT risks given the ubiquity of information technology in their operations as they become more digital.

ERM is the continuous process of identifying, analyzing, evaluating and addressing risk exposures, including those related to information systems, to mitigate their negative effects.

Enterprise Risk Management « ERM » is a methodological process that extends the domain of risk management to the strategic level of the organization, to guard against risks and other potential damages that may interfere with the organization's operations and objectives.

The ERM process and the internal audit function are intimately linked, with the latter's role being to provide objective assurance to the board of directors on the effectiveness of ERM activities. In order to understand this linkage, we have tried to study how internal audit proceeds to improve the ERM process.

Keywords: information systems, operational risks, risk management, ERM process, internal audit, performance.