MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

ÉCOLE SUPERIEURE DE COMMERCE

MÉMOIRE

de fin de cycle en vue de l'obtention du diplôme de master en sciences de gestion

Spécialité : Contrôle de gestion

Thème :

Audit du processus de gestion des risques opérationnels liés aux système d'information
Cas : Banque Nationale d'Algérie (BNA)

Présenté par :

BENDJEBLA Nesrine

Encadré par :

Pr OUDAI Moussa

Professeur en sciences de gestion à l'ESC

Lieu de stage : la Banque nationale d'Algérie (BNA)
Période de stage : Du 22 /02/2024 au 27/05/2024

Année universitaire : 2023/2024

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR

ET DE LA RECHERCHE SCIENTIFIQUE

ÉCOLE SUPERIEURE DE COMMERCE

MÉMOIRE

de fin de cycle en vue de l'obtention du diplôme de master en sciences de gestion

Spécialité : Contrôle de gestion

Thème :

Audit du processus de gestion des risques opérationnels liés aux système d'information

Cas : Banque Nationale d'Algérie (BNA)

Présenté par :

BENDJEBLA Nesrine

Encadré par :

Pr OUDAI Moussa

Professeur en sciences de gestion à l'ESC

Lieu de stage : la Banque nationale d'Algérie (BNA)

Période de stage : Du 22 /02/2024 au 27/05/2024

Année universitaire : 2023/2024

REMERCIEMENTS

Au nom d'Allah, le Tout-Miséricordieux, le Très-Miséricordieux,
En ce moment solennel, je rends grâce à Allah, le guide ultime, pour m'avoir accordé la force, la persévérance et la sagesse nécessaires à la réalisation de ce mémoire de fin d'études

En ce moment solennel, je tiens à exprimer ma profonde gratitude envers ceux qui ont contribué de manière significative à la réalisation de ce mémoire de fin d'études.
Je voudrais tout d'abord adresser mes sincères remerciements à mon encadreur, Monsieur Oudai Moussa, dont les conseils éclairés, la patience et l'engagement ont joué un rôle crucial dans la réussite de ce travail. Sa guidance constante a été une source d'inspiration et a grandement enrichi mon expérience académique.

Un merci chaleureux à l'équipe pédagogique de mon école, en particulier aux enseignants qui m'ont transmis leur savoir et leur passion tout au long de mon parcours. Leurs enseignements ont été un pilier essentiel pour la construction de mes connaissances.

Je tiens également à exprimer ma reconnaissance envers l'équipe de stage qui m'a accueilli avec bienveillance. Leur expertise et leur coopération ont grandement contribué à l'enrichissement de mon apprentissage pratique.

Enfin, un immense merci à Madame Lhachemi Lamia, dont le soutien indéfectible et les conseils avisés ont été d'une valeur inestimable tout au long de la réalisation de ce mémoire.
Que chacun de vous trouve ici l'expression sincère de ma gratitude et de ma reconnaissance. Puissiez-vous être récompensés abondamment pour votre contribution à la réussite de ce travail.
Que la paix et les bénédictions d'Allah soient sur vous tous.

DEDICACES

À mon père bien-aimé, Karim Bendjebla, et à ma mère exceptionnelle, Hafida Ghettas, dont l'amour inconditionnel a illuminé chaque étape de ma vie. Votre dévouement et vos sacrifices ont été une source infinie d'inspiration, et je suis profondément reconnaissante de la force que vous m'avez transmise.

À mes chères sœurs, Meriem et Hiba, et à mon frère, Merouan, qui ont partagé avec moi rires, peines et triomphes. Votre présence a été un précieux cadeau, et nos liens familiaux sont les joyaux qui embellissent ma vie.

À toute la famille, vous êtes les racines qui me donnent la force de grandir et les ailes qui me permettent de rêver. Chacun de vous a contribué à ma croissance, et je suis reconnaissante pour les moments de bonheur partagés.

Que cette dédicace soit une humble expression de ma gratitude envers chacun d'entre vous. Que les liens familiaux continuent à se fortifier, et que l'amour qui nous unit demeure éternel.

Avec tout mon amour.

SOMMAIRE

LISTE DES ABREVIATIONS

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 d'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 Organizations

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 Executives 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 Entreprise
USB : Universal Serial Bus

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ANNEXES

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

Cas : Banque Nationale d'Algérie (BNA)

RÉSUMÉ

Les entreprises sont actuellement confrontées à une diversité de risques qui pourraient compromettre leur stabilité et leur expansion, notamment les risques informatiques, en raison de la généralisation des technologies de l'information dans leurs opérations, à mesure qu'elles se numérisent.

La gestion des risques informatiques représente un processus ininterrompu d'identification, d'analyse, d'évaluation et de traitement des expositions aux risques, en particulier ceux associés aux systèmes d'information, dans le but d'atténuer leurs conséquences négatives.

L'Enterprise Risk Management (ERM) est une méthodologie qui élargit le champ de la gestion des risques au niveau stratégique de l'organisation, visant à se prémunir contre les risques et autres dommages potentiels qui pourraient entraver ses opérations et objectifs.

Le processus ERM et la fonction d'audit interne sont étroitement liés, cette dernière ayant pour mission de fournir une assurance objective au conseil d'administration quant à l'efficacité des activités de l'ERM. Pour appréhender cette relation, nous avons entrepris d'étudier comment l'audit interne contribue à l'amélioration du processus de gestion des risques liés aux systèmes d'information.

Mots-clés : systèmes d'information, risques opérationnels, management des risques, processus ERM, audit interne, performance.

Audit of the Operational Risk Management Process Related to Information Systems
Case of the National Bank of Algeria (BNA)

ABSTRACT

Businesses are currently facing a variety of risks that could compromise their stability and growth, especially in the realm of IT risks due to the widespread use of information technologies in their operations as they undergo digital transformation.

The management of IT risks represents an ongoing process of identification, analysis, evaluation, and treatment of risk exposures, particularly those associated with information systems, with the aim of mitigating their negative consequences.

Enterprise Risk Management (ERM) is a methodology that broadens the scope of risk management to the strategic level of the organization, seeking to safeguard against risks and other potential damages that could hinder its operations and objectives.

The ERM process and the internal audit function are closely intertwined, with the latter tasked with providing an objective assurance to the board of directors regarding the effectiveness of ERM activities. To comprehend this relationship, we have undertaken a study on how internal audit contributes to enhancing the process of managing risks associated with information systems.

Keywords : information systems, operational risks, risk management, ERM process, internal audit, performance.

تدقيق عملية إدارة المخاطر التشغيلية المتعلقة بأنظمة المعلومات
حالة البنك الوطني الجزائري

الملخص

الشركات تواجه حاليًا مجموعة من المخاطر التي قد تعرض استقرارها وتوسعها للتهديد، وخاصة مخاطر تكنولوجيا المعلومات نتيجة لانتشار تلك التقنيات في عملياتها، مع تقدمها نحو الترقيم الرقمي . إدارة مخاطر تكنولوجيا المعلومات تمثل عملية مستمرة لتحديد وتحليل وتقييم ومعالجة التعرض للمخاطر، خاصة تلك المتعلقة بأنظمة المعلومات، بهدف التخفيف من تداولاتها السلبية .إدارة المخاطر الشاملة هي منهجية توسع نطاق إدارة المخاطر إلى المستوى الاستراتيجي للمؤسسة، بهدف الوقاية من المخاطر والأضرار الأخرى المحتملة التي قد تعيق عملياتها وأهدافها .عملية الإدارة الشاملة ووظيفة التدقيق الداخلي مرتبطتان ارتباطًا وثيقًا، حيث تتولى الأخيرة مهمة توفير ضمان موضوعي لمجلس الإدارة بشأن فعالية أنشطة الإدارة الشاملة. لفهم هذا الارتباط، قمنا بدراسات كيفية مساهمة التدقيق الداخلي في تحسين عملية إدارة المخاطر المتعلقة بأنظمة المعلومات

كلمات مفتاحية: أنظمة المعلومات، مخاطر تشغيلية، إدارة المخاطر، عملية الإدارة الشاملة، التدقيق الداخلي، الأداء

INTRODUCTION GENERALE

INTRODUCTION GENERALE

De plus en plus confrontées aux problématiques de risques, les entreprises sont progressivement devenues sensibles à la nécessité d'une gestion efficace des risques ;

Mais les risques sont de diverses natures. Dans ce travail nous nous intéressons aux risques liés aux systèmes d'informations. À l'ère numérique actuelle, les systèmes d'information constituent le cœur névralgique de toute entreprise moderne. Ils sont le moteur de l'efficacité opérationnelle, de l'innovation, de la prise de décision et de la compétitivité sur le marché. Toutefois, cette dépendance croissante à l'égard des systèmes d'information s'accompagne d'une complexité et de risques considérables. L'interruption d'un système, la divulgation non autorisée de données sensibles ou la vulnérabilité aux cyberattaques peuvent avoir des conséquences désastreuses sur l'ensemble de l'organisation.

Dans ce contexte, la gestion des risques liés aux systèmes d'information revêt une importance cruciale. Elle s'inscrit dans le cadre plus vaste de l'Enterprise Risk Management (ERM), une approche stratégique et holistique visant à identifier, évaluer et gérer l'ensemble des risques auxquels une organisation est exposée. L'ERM reconnaît que les systèmes d'information sont un actif vital, mais qu'ils sont également une source significative de risques potentiels.

L'objectif de ce mémoire est d'explorer en profondeur la dynamique complexe entre les systèmes d'information et les risques qui leur sont associés, en se concentrant sur le rôle central de la gestion des risques et de l'audit dans cette équation. Nous analyserons les enjeux majeurs liés à la protection, à la disponibilité et à l'intégrité des systèmes d'information, tout en tenant compte de l'évolution constante de la technologie et de l'environnement réglementaire.

Le concept d'ERM est essentiel à cette compréhension, car il offre un cadre conceptuel qui permet à une organisation de hiérarchiser et de gérer l'ensemble de ses risques de manière stratégique. Dans ce cadre, la gestion des risques liés aux systèmes d'information devient une composante intégrée de la gestion des risques globale de l'entreprise.

Au cours des prochains chapitres, nous aborderons en détail les principes fondamentaux de la gestion des risques liés aux systèmes d'information, les normes et les meilleures pratiques qui guident cette discipline, ainsi que les défis opérationnels et stratégiques que rencontrent les organisations dans ce domaine. En fin de compte, nous fournirons des recommandations pour

une gestion efficace des risques liés aux systèmes d'information, qui contribueront à renforcer la résilience et la compétitivité des organisations dans un environnement en perpétuelle évolution.

Objectifs recherchés :

- Examiner en profondeur les menaces et vulnérabilités spécifiques aux systèmes d'informations
- Étudier comment l'approche holistique de l'ERM peut renforcer la capacité de l'entreprise à anticiper et répondre aux risques opérationnels informatiques.
- Renforcer le rôle de l'audit interne pour assurer une surveillance continue des risques informatiques, détecter précocement les anomalies et contribuer à l'amélioration des contrôles.

Intérêt du sujet :

Le sujet traité présente un intérêt majeur dans le contexte actuel des entreprises en raison de la prévalence croissante des menaces numériques. En se focalisant sur les risques informatiques, cette étude offre une opportunité cruciale pour renforcer la résilience organisationnelle face aux cybermenaces et assurer la protection des actifs numériques essentiels.

L'intégration de l'Enterprise Risk Management (ERM) et l'amélioration du rôle de l'audit interne visent à créer un cadre stratégique favorisant la conformité aux normes internationales et la mise en place d'une culture d'amélioration continue.

L'approche pratique, illustrée par une étude de cas, offre des enseignements spécifiques permettant une application ciblée des solutions, renforçant ainsi la posture de sécurité et la capacité à anticiper les défis liés aux risques opérationnels informatiques. En résumé, ce sujet présente un intérêt crucial pour les organisations cherchant à fortifier leur sécurité opérationnelle dans un paysage numérique dynamique.

Raisons du choix du sujet :

- Comprendre et atténuer les risques opérationnels dans les systèmes d'information est crucial pour maintenir l'intégrité, la confidentialité et la disponibilité des données sensibles. Ce sujet s'aligne sur les priorités stratégiques visant à assurer la continuité des activités et à protéger les actifs organisationnels.
- Avec la numérisation croissante des opérations, la prévalence des menaces cybernétiques constitue un défi majeur. Se concentrer sur l'audit de la gestion des

risques opérationnels liés aux systèmes d'information répond à une problématique pressante pour les organisations modernes.

- L'inclusion des principes de l'Enterprise Risk Management (ERM) témoigne de l'engagement à adopter des pratiques exemplaires holistiques et internationalement reconnues. Cette intégration garantit une approche complète de la gestion des risques allant au-delà des mesures isolées.

Etudes antérieures :

- REMADNIA Hana, le rôle de l'audit interne dans la gestion des risques opérationnels, Mémoire de fin de cycle, École Supérieure de Commerce, 2017/2018
- Mémoire de fin d'études en vue de l'obtention du diplôme de master en sciences financières et comptabilité Le Système d'information Bancaire élaboré par MOHAND SAIDI Assia et YAHIATENE Saïd ; promo 2018 au niveau UNIVERSITE MOULOUD MAMMERI TIZI-OUZOU FACULTE DES SCIENCES ECONOMIQUES, COMMERCIALES ET DES SCIENCES DE GESTION DEPARTEMENT DES SCIENCES DE GESTION
- CHETOUI Mohammed Fath Eddine, La Gestion des risques opérationnels dans les activités bancaires, École Supérieure de Commerce, 2017/2018

Problématique :

Ce mémoire a pour ambition de fournir un aperçu complet et pragmatique de la gestion des risques liés aux systèmes d'information au sein du cadre de l'ERM, en intégrant les dernières avancées et les meilleures pratiques. En reconnaissant que les systèmes d'information sont à la fois une source de valeur et de vulnérabilité, nous aspirons à soutenir les décideurs, les professionnels de la gestion des risques et les auditeurs dans leur quête pour atteindre un équilibre optimal entre l'innovation et la sécurité.

Pour cela je dois 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, il est jugé utile de répondre aux questions secondaires suivantes :

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

- Quelles sont les méthodes et référentiels promettant la gestion des risques de SI ?
- Comment l'audit interne procède-t-il pour améliorer l'efficacité du processus d'Enterprise Risk Management (ERM) au sein des organisations ?

Hypothèses :

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

- **Hypothèse 1 :** Les risques opérationnels liés à la mise en place d'un SI varient en fonction de la taille de l'entreprise, de son secteur d'activité et de la complexité de ses processus.
- **Hypothèse 2 :** L'implication active des parties prenantes, y compris la direction, les responsables informatiques et les équipes de gestion des risques, est cruciale pour le succès de la gestion des risques de SI.
- **Hypothèse 3 :** L'indépendance de l'audit interne par rapport à d'autres fonctions de l'organisation favorise une évaluation objective et une influence positive sur l'ERM.

Méthodologie de recherche :

Afin de vérifier la véracité de mes hypothèses et répondre à ma problématique, cette étude est divisée en trois chapitres.

Le premier chapitre qui constituera le cadre théorique de l'étude va me 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 risque opérationnels ,à l'audit interne et au rôle qu'il joue dans le management des risques. J'ai aussi porté 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.

Les deux chapitres suivants comportent 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 selon la norme ISO 27001 dans la troisième section .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 hypothèse émises précédemment dans la dernière section, après avoir présenté la méthodologie de travail dans la seconde section.

Plan de recherche :

Afin d'apporter des éléments de réponse à ma problématique, mon travail sera structuré en trois chapitres :

Le premier chapitre : Explore les bases de la gestion des risques liés aux systèmes d'information, couvrant le système d'information organisationnelle, les risques opérationnels

Deuxième chapitre : Introduit l'Enterprise Risk Management et souligne le rôle vital de la fonction d'audit. Explore le processus ERM selon ISO 31000, la relation avec le contrôle interne, et l'apport spécifique de l'audit interne.

Troisième chapitre : Se concentre sur l'évaluation du processus de management des risques, en utilisant la BNA comme cas concret. Présente la méthodologie employée, analyse les résultats, identifie les points forts et les opportunités d'amélioration.

CHAPITRE I

Gestion des risques opérationnels des systèmes d'information

CHAPITRE I : GESTION DES RISQUES OPERATIONNELS DES SYSTEMES D'INFORMATON

L'évolution complexe et concurrentielle de l'environnement des entreprises actuelles confère aux informations un statut d'actif crucial, nécessitant valorisation et sécurisation. Les systèmes d'information répondent à ce besoin vital en traitant les flux d'informations croissants, assurant ainsi le développement et la pérennité des organisations.

Toutefois, la mise en place de tels systèmes peut entraîner des défis entravant leur implémentation, les risques émergents étant loin d'être négligeables. C'est pourquoi une gestion efficace des risques liés aux systèmes d'information et à l'utilisation des technologies de l'information s'avère plus que jamais essentielle.

Ce premier chapitre vise à familiariser avec la notion de système d'information et les concepts qui lui sont associés, tout en explorant la nature du risque, particulièrement le risque opérationnel et ses différentes typologies. Enfin, la dernière section examine les risques opérationnels liés aux systèmes d'informations, ainsi que les référentiels et méthodes pertinents pour leur traitement, soulignant l'importance d'une gestion efficace des risques au sein des entreprises.

SECTION 01 : LE SYSTEME D'INFORMATION ORGANISATIONNELLE

En tant que discipline axée sur les systèmes d'informations, cette approche accorde une attention particulière aux rôles cruciaux que jouent les informations dans le fonctionnement des organisations. Qu'il s'agisse d'informations à vocation commerciale, comptable ou fiscale, leur traitement revêt une importance stratégique. La qualité de ces informations, caractérisée par leur fiabilité, pertinence et précision, est cruciale pour la prise de décisions éclairées. Cette section explore la notion de système d'informations, ses différents types, ses dimensions et son rôle fondamental au sein de l'organisation.

1. L'entreprise système :

Dans l'étude de l'approche systémique, Yatchinovsky (2005) la définit comme une approche globale qui offre une vision d'ensemble d'un système en considérant ses éléments dans leur globalité. Cette approche se concentre sur les interactions entre ces éléments plutôt que sur une analyse détaillée de chacun d'eux.

Le biologiste Bertalanffy, cité par Yatchinovsky (2005), est reconnu comme le pionnier ayant introduit la réflexion sur la notion de système. Il a démontré l'importance de considérer un organisme dans sa totalité, mettant en avant sa complexité et sa dynamique propre, s'opposant ainsi à l'approche classique caractérisée par sa tendance réductrice.

L'analyse systémique, présentée comme une approche alternative à la logique cartésienne, rappelle également que tout système repose sur un ensemble de caractéristiques qui permettent d'établir une typologie des systèmes.

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

- **L'Interaction :** Il s'agit de la relation entre deux éléments avec une action réciproque. Cette double action souligne l'importance des influences mutuelles entre les composants d'un système.

- **La Totalité :** Un système ne se réduit pas à la somme de ses éléments. Comprendre le tout est essentiel, car connaître les parties sans connaître l'ensemble, ou vice versa, est impossible.

- **L'Organisation :** Dans le contexte du modèle systémique, il s'agit de l'agencement des relations entre les individus ou des processus. Cet agencement permet d'assembler et de mettre en œuvre la matière, l'énergie et l'information.

- **La Complexité** : Présente dans tous les systèmes, la complexité est une caractéristique nécessaire à conserver. Elle souligne la diversité et l'interconnectivité des éléments au sein d'un système.

1.2. L'entreprise en tant que système :

Un système : un ensemble de procédés, de pratiques organisées, destiné à assurer une fonction définie. » (LAROUSSE en ligne, s. d.)

Jean-Louis Le Moigne propose cinq critères pour définir un système, le considérant principalement comme un objet réel que l'on cherche à modéliser, représenter et anticiper son

comportement par le biais de simulations. Ce système, en interaction avec son environnement et d'autres systèmes, vise à réaliser un profit grâce à une activité créatrice de valeur ajoutée, orchestrée par ses acteurs et des flux organisés selon sa structure (M. Gillet, P. Gillet, 2010).

Initialement appliqué en biologie pour expliquer les relations au sein d'un organisme vivant, le concept de système s'étend désormais au domaine de l'entreprise, défini comme un ensemble intégré de composantes ou de sous-systèmes travaillant conjointement vers un objectif commun (Bursh et Felix, 1984).

Dans l'ensemble, un système est caractérisé comme un ensemble complexe d'éléments organisés et interagissant pour atteindre un objectif spécifique. On distingue les systèmes fermés, isolés et sans échanges d'informations avec l'environnement, des systèmes ouverts en interaction constante avec leur milieu.

L'entreprise, apparue au 16ème siècle, est décrite comme un ensemble dynamique d'éléments en interaction, organisé autour d'un but précis (De Rosnay, 1975). L'Institut National De La Statistique Et Des Études Économiques la définit comme une unité économique juridiquement autonome produisant des biens ou des services pour le marché.

Conceptuellement, l'entreprise se présente comme une institution guidée par un plan d'action visant à créer des biens et services pour les usagers. Elle combine et consomme diverses ressources (matérielles, humaines, financières, immatérielles et informationnelles) selon une direction prédéfinie (Tawfik et Chauvel, 1980).

Pour déterminer et distinguer une entreprise des autres entités économiques, plusieurs critères doivent être pris en compte :

- Elle exerce ses activités sur des marchés, combine de manière efficiente les facteurs de production, et coordonne les comportements individuels au sein d'une structure hiérarchique en tant qu'entité productive.
- Elle jouit d'une autonomie juridique dans ses prises de décision.
- Elle représente le cadre de l'activité entrepreneuriale, où l'entrepreneur prend des risques et innove.

L'entreprise, en tant que réalité socio-économique, doit choisir une forme juridique spécifique pour son existence légale et son développement, telles que l'entreprise individuelle, l'EURL, etc. Elle procède à son enregistrement auprès des autorités compétentes, notamment au Registre du commerce. Dans une perspective systémique, l'entreprise est envisagée comme un ensemble de sous-systèmes interagissant, identifiés selon divers critères tels que la fonction, la nature des flux, les niveaux, etc. Ces sous-systèmes échangent des flux de matières, de finances ou d'informations, et leur organisation vise à assurer la réalisation des activités et des objectifs de l'organisation. Ainsi, l'entreprise est considérée comme un système ouvert, finalisé et régulé.

Il semble que le schéma suivant, décrivant la décomposition de l'entreprise en trois sous-systèmes :

Figure(01) : les sous-systèmes

2. Le système d'information

Bien que couramment associée à la dimension technologique par l'utilisation d'ordinateurs et de réseaux, la notion de Système d'Information (SI) va au-delà et englobe simultanément les dimensions informationnelles, technologiques et organisationnelles.

R. Mason et I. Mitroff (cités par Morley et al., 2011) soulignent le rôle crucial de l'information dans l'organisation en définissant un système d'information comme englobant au moins une personne ayant un besoin spécifique d'éléments présentés de manière adaptée au contexte organisationnel. Dans cette optique, le système d'information s'intègre au processus décisionnel, offrant un soutien précieux au décideur.

G. Davis et M. Olson (cités par Morley et al. 2011), en considérant l'ensemble des activités organisationnelles, décrivent le système d'information comme un mécanisme générant de l'information, grâce à la relation intégrée entre l'utilisateur et la machine, bénéfique à la prise de décision humaine et à l'exécution des tâches. Cette définition demeure toutefois limitée à la dimension informationnelle.

En résumé, un système d'information représente un ensemble structuré de ressources matérielles et logicielles, d'acteurs ou utilisateurs, de pratiques de travail, de données et de réseaux, visant à collecter, traiter, mémoriser et transmettre l'information sous différentes formes pour répondre aux besoins de l'organisation (Reix et al., 2016).

Ainsi, le système d'information englobe l'ensemble des flux d'informations circulant à l'intérieur de l'organisation et avec son environnement externe, associé aux moyens déployés pour les gérer en vue d'atteindre des objectifs stratégiques alignés sur la stratégie globale de l'entreprise ainsi que des objectifs opérationnels spécifiques. Ces derniers se matérialisent à travers les fonctions du SI, incluant la collecte/saisie, le stockage, la transformation/traitement, la diffusion/communication de l'information (Reix et al. 2016).

2.1. Types de systèmes d'information :

Un Système d'Information (SI) au sein d'une organisation peut être subdivisé en trois catégories correspondant aux niveaux stratégique, de gestion et opérationnel de l'organisation. De manière similaire, une approche fonctionnelle peut être adoptée en considérant quatre domaines : vente et marketing, fabrication et logistique, finance et comptabilité, ressources humaines. Ces systèmes sont conçus pour assister les responsables et les équipes dans leurs processus décisionnels et d'exécution en fournissant les informations nécessaires à l'organisation pour l'atteinte de ses objectifs (K. et J. Laudon, 2010).

2.1.1. Selon les niveaux organisationnels :

- Le niveau des opérations :

Les systèmes opérationnels (SO) jouent un rôle crucial dans le soutien des opérations quotidiennes d'une organisation. Ils sont également appelés systèmes de traitement des transactions (STT) et sont chargés d'exécuter et d'enregistrer les transactions de base, telles que la saisie des bons de commandes. Les STT traitent à la fois les opérations internes et externes, générant ainsi des informations essentielles pour d'autres systèmes. Leur bon fonctionnement est vital, car toute défaillance peut entraîner des risques importants pour l'organisation.

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…

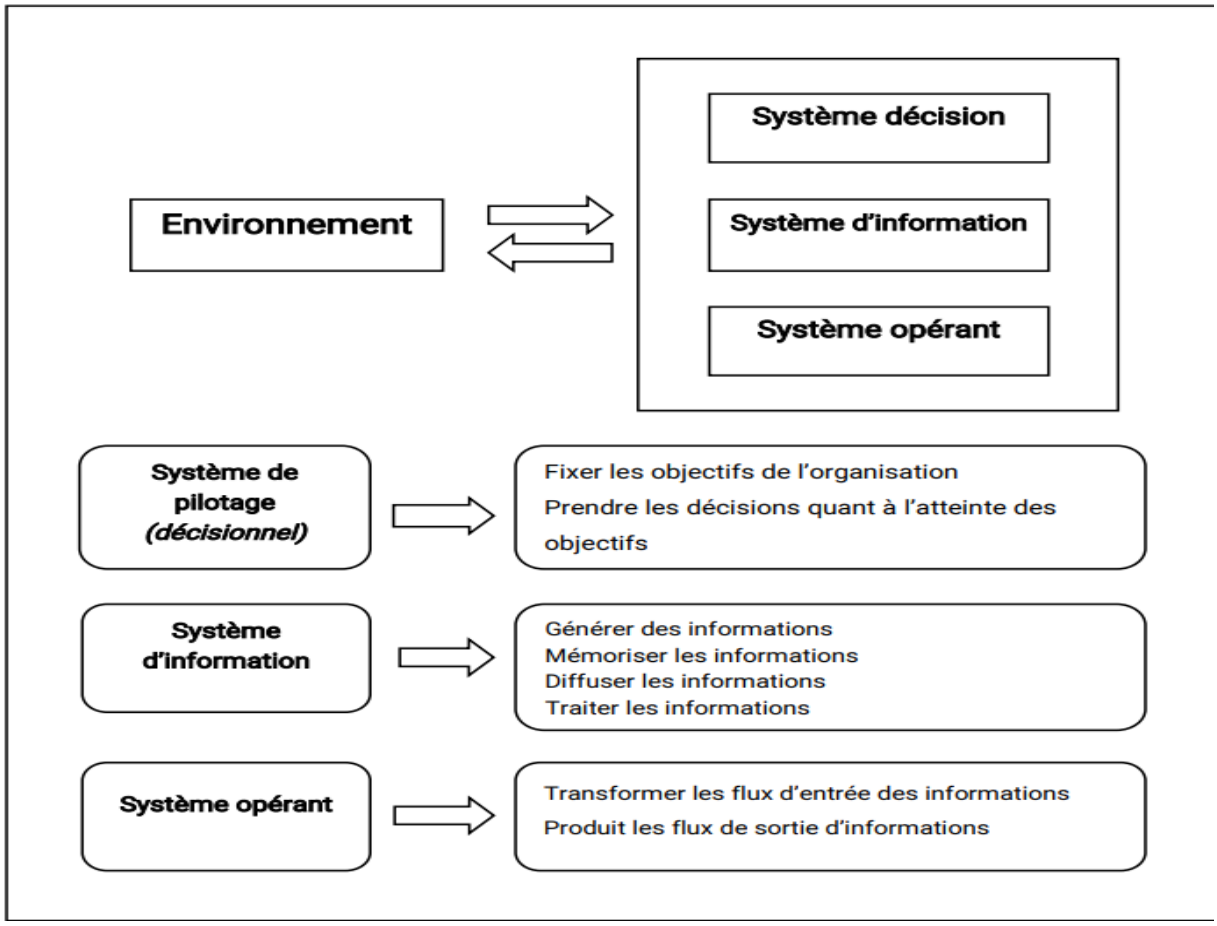
Tableau 01 : Exemples de systèmes de traitement des transactions (STT)

Source : inspiré de "Management des systèmes d'information" de Laudon K. et J. et al. (2010), pp. 53 à 55. Paris : Pearson.

- **Le niveau de la gestion :**

Les systèmes de management opérationnel (SMO) sont des systèmes qui transforment les informations opérationnelles en rapports périodiques, fournissant ainsi un support essentiel aux cadres responsables pour coordonner et piloter l'activité de l'entreprise.

Ces systèmes se subdivisent en deux catégories : les systèmes d'information de gestion (SIG) et les systèmes d'aide à la décision (SAD). Les SIG utilisent les données internes des systèmes de traitement des transactions (STT) pour générer des rapports périodiques, facilitant ainsi aux cadres intermédiaires la réponse aux questions routinières selon des procédures prédéfinies. Les SAD, quant à eux, regroupent les données des STT et les résultats des SIG, en plus d'informations externes, pour formuler des rapports spéciaux utiles aux cadres intermédiaires et aux experts.



Dotés de puissantes capacités analytiques pour traiter d'importantes quantités de données manipulables, les SAD permettent aux gestionnaires d'obtenir des détails approfondis sur une situation, favorisant ainsi l'optimisation de la planification, la prise de décisions, l'atteinte des objectifs et la supervision des opérations. La comparaison entre les résultats des SAD et des SIG aide les cadres supérieurs à perfectionner le processus décisionnel pour des résultats plus aboutis.

- Le niveau stratégique :

Les systèmes d'informations stratégiques (SIS) jouent un rôle crucial dans la prise de décision par la direction. Ils prennent forme à travers des systèmes conçus pour assister les dirigeants dans la gestion globale de l'organisation, appelés Systèmes d'Information pour les Dirigeants (SID).

Ces systèmes intègrent, en plus des données externes, les informations traitées et résumées par les Systèmes d'Information de Gestion (SIG) et les Systèmes d'Aide à la Décision (SAD). Ces données sont filtrées et transformées en graphiques par les SID, accessibles via une interface

web. Ils sont utilisés pour réduire les incertitudes décisionnelles liées à l'avenir de l'entreprise et pour améliorer les perspectives et les performances globales de l'organisation.

2.1.2. Selon un point de vue fonctionnel :

- **Les systèmes de vente et de marketing :** regroupent les données de chaque niveau de l'organisation pour un pilotage optimal des activités commerciales, incluant les clients potentiels, les études de marché et la concurrence.
- **Les systèmes de fabrication et de logistique :** tels que le Système d'Information de Gestion de Cycle de Vie d'un Produit (GCVP), sont essentiels pour les entreprises industrielles. Ils permettent de réduire les coûts liés au prototypage, de gérer les approvisionnements, d'exécuter les commandes et de gérer les changements relatifs.
- **Les systèmes des activités financières et comptables :** sont dédiés à l'établissement de prévisions à long terme, à la gestion des ressources financières et au suivi des mouvements de fonds au sein de l'entreprise.
- **les systèmes des ressources humaines** : s'occupent de la tenue de dossiers complets et de la création de programmes pour la main-d'œuvre, couvrant des aspects tels que le recrutement, le perfectionnement et le maintien du personnel.

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

L'intégration dans les Systèmes d'Information (SI) vise à regrouper, transformer et présenter rapidement les données de l'ensemble des systèmes, en éliminant les activités superflues. Elle assure la cohérence, la communication et la synchronisation pour éliminer les inefficacités telles que la recherche, la saisie et la transmission répétitives des informations.

Un SI intégré dans une entreprise coordonne l'ensemble des processus et actions avec ses partenaires (fournisseurs, clients), en regroupant les informations de tous les domaines fonctionnels. Cette démarche répond à la nécessité de réactivité et d'obtention rapide d'informations fiables, en éliminant les systèmes isolés.

Pour une intégration réussie, une communication codifiée propre à l'organisme est essentielle, garantissant une information pertinente, structurée et cohérente (Tassin, 2005).

2.2.1. Les pratiques d'intégration :

L'intégration d'un Système d'Information (SI), selon Thevenot (2011), doit être envisagée comme un mode d'organisation logique. Elle repose sur l'utilisation d'outils et de technologies tels que les Progiciels de Gestion Intégrés (PGI/ERP), modulaires et reposant sur une base de données unique, considérée comme le pivot du système. Les PGI se déclinent en modules génériques (comptabilité, contrôle de gestion, ressources humaines), industriels (planification, ordonnancement) et destinés aux services. L'intégration d'applications d'entreprise (IAE) se fait par le biais de middleware, préservant ainsi l'existant du SI.

Les entrepôts de données (Data Warehouse) sont essentiels pour la mise en cohérence et l'intégration des données, reposant sur leur structuration, historisation et traçabilité. L'architecture orientée services (AOS) vise à améliorer la flexibilité opérationnelle du SI en optimisant l'utilisation des ressources existantes, minimisant les coûts de développement et de déploiement des nouvelles applications. L'AOS facilite l'adaptation aux évolutions du métier de l'entreprise et de son environnement en modélisant et mutualisant les processus métiers majeurs (Thevenot, 2011).

2.3.Dimension d'un SI :

Pour mieux appréhender la notion de système d'information, il est crucial de le concevoir comme un système multidimensionnel composé de trois dimensions distinctes (Reix et al., 2016).

2.3.1. Une dimension informationnelle/management :

Les systèmes d'information fournissent aux responsables des informations spécifiques et pertinentes pour influencer leurs décisions. Leur objectif premier est de représenter ces informations de manière pertinente et de qualité. La communication et le partage des connaissances sont cruciaux dans ce processus, mais peuvent présenter des risques de distorsion. Il est donc essentiel que les informations répondent aux besoins des utilisateurs. La valeur et le coût associés à l'obtention de l'information sont également importants à considérer.

2.3.2. Une dimension technologique :

Les systèmes d'information reposent sur une architecture technologique qui exploite diverses

Technologies numériques pour acquérir, stocker, traiter et communiquer des informations sous forme de données symbolisées. Cette infrastructure comprend du matériel informatique (postes de travail, serveurs) et des télécommunications. L'informatisation des SI a permis de réduire le temps de traitement des données et l'espace qu'elles occupent, facilitant leur utilisation, leur modification et leur transport. Elle assure la connectivité et la mobilité, permettant l'accès aux données depuis différents endroits interconnectés.

2.3.3. Une dimension organisationnelle :

Pour un système d'information au sein d'une organisation, son aspect organisationnel se décline en deux perspectives : le fonctionnement, englobant les activités, événements et résultats des processus ainsi que leur coordination, et la structure, intégrant la gestion commerciale et marketing grâce à l'information destinée aux gestionnaires et à la gestion des connaissances.

2.4. Rôles et moyens d'un SI :

Le rôle d'un système d'information, se résume en trois points clés : (M. et P. Gillet (2010))

- il s'agit comme un instrument de couplage entre les modules opérationnels et les modules pilotes au sein de l'organisation, favorisant une prise de décision efficace et une réaction rapide aux changements environnementaux.
- il facilite la communication interne et externe, préservant ainsi l'histoire, le savoir et le savoir-faire de l'entreprise.
- il transforme les données pour les adapter aux besoins de l'entreprise et les fait circuler conformément aux exigences des destinataires. En somme, le système d'information contribue à améliorer la productivité en permettant au système opérant de communiquer des informations collectées et modifiées au système de pilotage.

2.4.1. Les moyens d'un SI :

M. et P. Gillet (2010) ont identifié les moyens suivants pour un système d'information :

- **Ressources humaines** : Les individus salariés de l'organisation sont la principale ressource, étant au centre de la création de l'information.

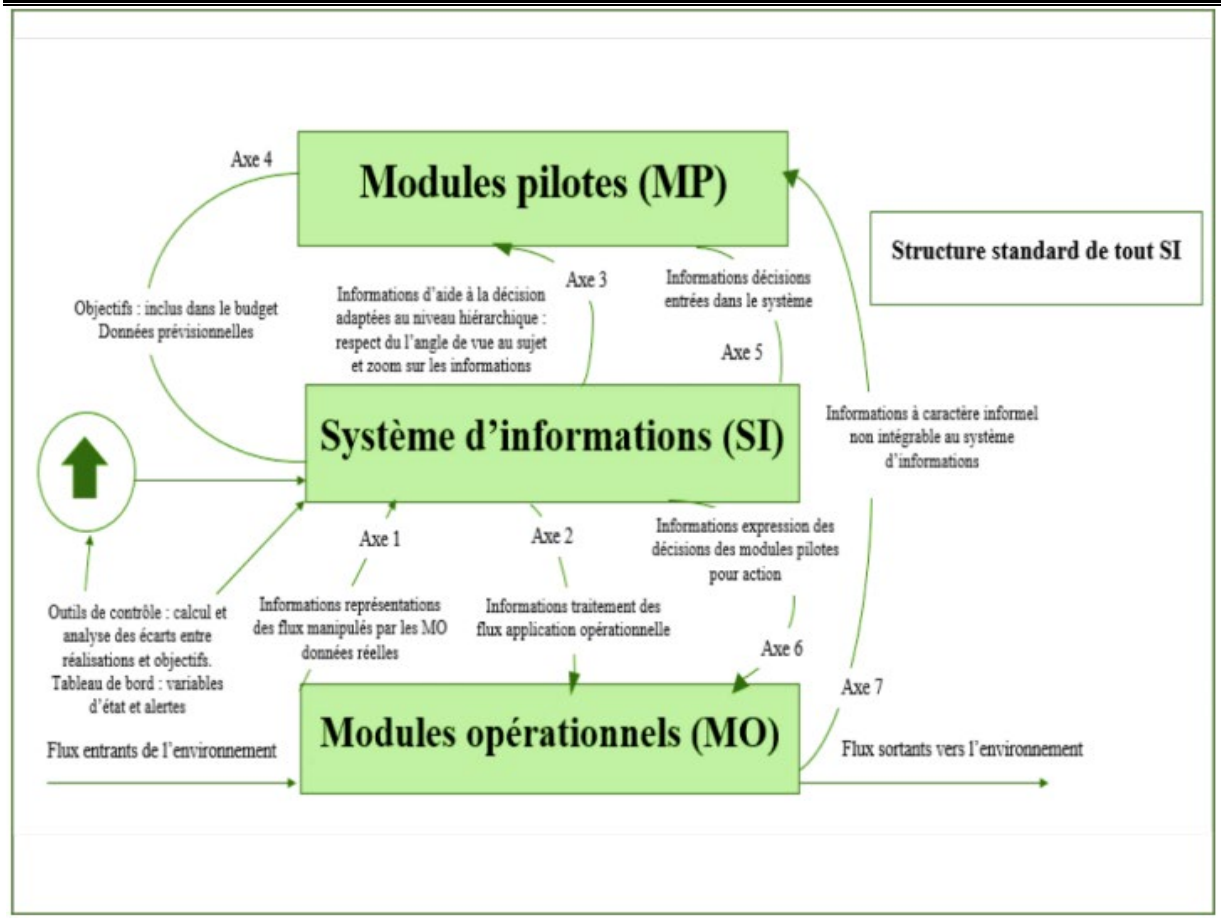
- **Ressources matérielles :** En compassant toute l'infrastructure technologique, y compris ordinateurs, moyens d'impression, serveurs, etc., ainsi que l'aménagement physique des espaces.
- **Ressources immatérielles :** Se référant à l'aspect logiciel du système d'information, comprenant l'ensemble de l'architecture applicative de l'organisation.
- **Ressources financières :** La gestion de l'information, bien que de nature immatérielle, peut être coûteuse, posant souvent des défis dans le calcul du retour sur investissement des technologies de l'information.

Le "paradoxe de Solow", souligné par le professeur Robert Solow, met en lumière le décalage croissant entre l'amélioration de la productivité des ordinateurs et celle des salariés. Cela résulte de l'écart temporel entre l'investissement en connaissances, la période de formation et les effets d'obsolescence. Les technologies de gestion de l'information demeurent cruciales pour les organisations, quel que soit leur coût.

2.5. Les caractéristiques d'un SI :

Il existe plusieurs interactions au sein du système d'informations pour répondre aux besoins de l'organisation. Ces interactions, présentées sous forme d'axes par M. et P. GILLET (2010), facilitent la circulation d'informations entre les modules opérationnels et les modules pilotes.

Figure(02) : Les flux d'information d'un SI à partir de « Système d'information des ressources humaines »



Source : 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, monétaires ou humains lors de leur transformation en flux sortants.
- ✓ 2ème axe se concentre sur le traitement des flux d'informations par le système d'informations, essentiel pour les modules opérationnels et pilotes. Les informations traitées, issues de la transformation des flux entrants en flux sortants, sont cruciales pour comparer les objectifs et orienter les décisions futures.
- ✓ Le 3ème axe souligne le rôle du SI dans la circulation rapide d'informations synthétiques et adaptées aux destinataires, favorisant une prise de décision efficace sans déformation.
- ✓ Le 4ème axe insiste sur l'intégration des objectifs prévisionnels par le SI, définis par le module pilote à travers la démarche budgétaire, assurant le contrôle et la mémorisation des buts à atteindre.

- ✓ Le 5ème axe met en lumière l'importance d'informer les acteurs opérationnels des décisions prises par les modules pilotes, soulignant la nécessité d'intégrer ces décisions dans le SI.
- ✓ Le 6ème axe souligne la capacité du SI à transformer les décisions globales en informations opérationnelles, nécessaires pour un couplage efficace entre les modules pilotes et opérationnels grâce à une structuration appropriée.
- ✓ Le 7ème axe aborde les informations informelles, soulignant que certaines données, par nature, circulent de manière informelle, sans intervention du SI, préservant ainsi leur caractère subjectif.

2.6. Qualités et limites d'un SI :

Les critères introduits par M. et P. GILLET (2010) pour l'évaluation des informations dans un système d'information incluent :

- **Rapidité et facilité :** La vitesse de transmission des informations est cruciale, dépendant du temps maximal tolérable pour que les décisions et les actions associées soient effectuées dans des délais compatibles, en tenant compte du moment et de la nature de l'information.
- **Fiabilité :** La fiabilité est une qualité essentielle, exigeant que l'information soit pertinente et complète lors de son acquisition, et qu'elle soit transmise sans déformation ni perte tout au long du circuit.
- **Intégrité :** Le système d'information maintient l'intégrité des informations, assurant qu'elles restent dans un état cohérent et permettant de réagir aux situations qui pourraient rendre les informations incohérentes.
- **Sécurité :** Le SI garantit la protection des informations en les sauvegardant en premier lieu et en anticipant les menaces extérieures par le biais de dispositifs tels que routeurs filtrants, antivirus, pare-feux et détecteurs d'intrusions.
- **Confidentialité :** Le SI assure la confidentialité des informations, mettant en place des moyens matériels et immatériels pour contrer l'espionnage industriel.

2.6.1. Ses limites :

Certaines informations subjectives liées aux relations humaines dans une organisation échappent au système d'information, bien qu'elles puissent être cruciales pour comprendre le fonctionnement. Ces données, non reproductibles et non codifiables, ne

peuvent être traitées automatiquement, mais doivent être prises en compte par les modules pilotes dans la prise de décision. Les outils informatiques permettent de traiter automatiquement certaines informations dans le système d'information, comme le traitement des commandes clients et fournisseurs, avec des procédures définies à l'avance. Il est crucial de différencier les domaines automatisables de ceux automatisés pour distinguer les données informatisées de celles soumises à un traitement manuel (M. et P. GILLET, 2010).

3. L'infrastructure technologique d'un SI :

L'optimisation de la performance opérationnelle d'une entreprise passe par des investissements dirigés par les managers, englobant les aspects matériels, logiciels et services associés, et impliquant les ressources humaines et techniques. (Référence : K. et J. Laudon et al. 2013)

3.1. Informatique, processus métier et SI :

Le système d'information ne doit pas être confondu avec le système informatique. Ce dernier représente seulement une partie du système d'information, englobant les moyens informatiques nécessaires au traitement de l'information. L'informatique, quant à elle, est définie comme la science du traitement automatique de l'information, englobant matériels et logiciels pour soutenir les connaissances et les communications. De nos jours, le terme "système informatique" est utilisé pour couvrir à la fois les aspects matériels et logiciels de l'infrastructure de l'information.

3.1.1. La distinction entre SI et informatique :

Tableau (02) : Distinctions entre informatique et système d'information à partir de « Le système d'information nouvel outil de stratégie »

Informatique	Système 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 de la construction du système informatique.	Il relève du domaine de l'entreprise dans son ensemble, et dans le cadre d'un projet, le maître d'ouvrage et le maître d'œuvre sont tous deux responsables de la définition et de la mise en œuvre du système d'information

Source :, Deyrieux A., 2004, p.12, Maxima.

3.1.2. Processus métier et SI :

Un processus, selon l'ISO 9000:2000, est un ensemble d'activités interconnectées transformant des éléments d'entrée en éléments de sortie. Morley et al. (2011) le caractérisent davantage comme un regroupement d'activités orienté vers les métiers et les systèmes d'information, offrant flexibilité et interprétation aux acteurs. Il implique des rôles, utilise des ressources et peut être conditionné par des événements internes ou externes.

Un processus métier, selon Morley et al., organise les opérations pour atteindre des objectifs définis par la stratégie, impliquant un ou plusieurs processus de système d'information. Les processus SIs, à leur tour, utilisent des activités logicielles, des machines et des objets informatiques pour effectuer des traitements informatiques spécifiques.

La modélisation des processus métiers et des processus SIs partage des similitudes, mais les processus informatiques nécessitent une formalisation plus poussée, notamment pour décrire les objets, les événements, les conditions et les traitements élémentaires.

Processus Principaux : Les processus principaux constituent le cœur de l'organisation, générant de la valeur et offrant des avantages stratégiques. Leurs résultats sont destinés à des clients ou partenaires externes, et ils nécessitent une modélisation détaillée. Cependant, ils ne sont pas facilement transposables entre différentes organisations.

Processus Secondaires : Les processus secondaires sont essentiels à l'exécution des processus principaux, mais ils ne contribuent pas directement à la création de valeur. Ils englobent des activités telles que les états comptables ou la paie. Ces processus peuvent s'adapter en cas d'intégration d'un progiciel, mais ils restent des sources de coûts.

Processus de Pilotage : Les processus de pilotage visent à contrôler l'atteinte des objectifs et la mise en œuvre de la stratégie organisationnelle. Souvent représentés par des tableaux de bord, ils incluent des aspects tels que le suivi des ventes, le taux de remplissage ou la gestion des réclamations. Un exemple concret est le processus qualité, assurant la bonne définition des autres processus .

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

K. et J. LAUDON (2010) ont identifié 7 composantes interconnectées que les entreprises devraient investir pour garantir cohérence et fiabilité à long terme. Voici une synthèse de ces composantes :

Tableau (03) : Composantes de l'infrastructure technologique d'un SI. Inspiré de « Management des systèmes d'information »

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.

Source : de Laudon K. et J. et al. (2013), pp. 174 à 178. Paris : Pearson.

SECTION 2 : LE RISQUE OPERATIONNEL D'UNE ENTREPRISE

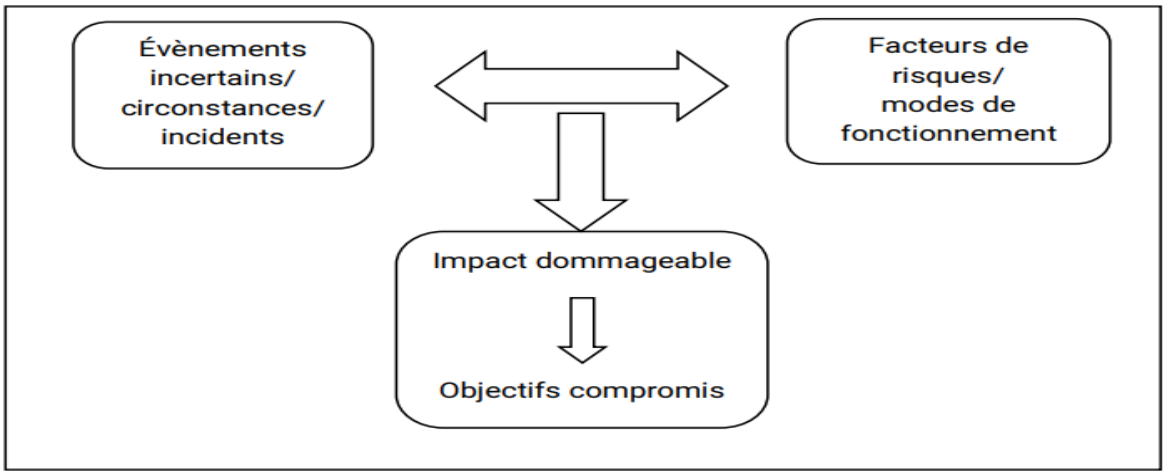
Aujourd'hui, la gestion des risques devient cruciale en entreprise, étant essentielle à sa pérennité et à sa croissance. Les risques opérationnels, issus du cœur opérationnel de l'entreprise, se présentent comme l'un des défis les plus complexes en raison de leur ampleur considérable. Dans cette section, nous explorerons les concepts fondamentaux liés au risque opérationnel

1. La notion du risque :

Le risque, selon l'IIA, est la possibilité d'un événement impactant la réalisation des objectifs. Pour l'IFACI, il représente un ensemble d'aléas pouvant avoir des conséquences négatives sur une entité, nécessitant le contrôle interne et l'audit pour assurer autant que possible la maîtrise. Larousse en ligne le décrit comme un danger ou inconvénient probable exposant à un préjudice, assuré par les compagnies d'assurances. Ces définitions soulignent les composantes du risque, à savoir la gravité des conséquences et la probabilité d'occurrence. L'ISO précise que le risque est la possibilité qu'un événement impacte les objectifs, mesuré en termes de conséquences et de probabilités. Schick ajoute que le risque est lié à l'atteinte d'un objectif et se définit comme la combinaison d'un événement incertain et d'un mode de fonctionnement aléatoire ayant pour conséquence le non-atteint d'un objectif.

Ce schéma résume la conceptualisation et la définition du risque :

Figure (03) : Conceptualisation et définition du risque. À partir de « Audit interne et référentiels de risque »



Source : de Schick et al. (2010). P. 11. Paris : Dunod.

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

Il existe des similitudes entre trois termes qui n'expriment pas les mêmes idées, générant souvent des confusions, notamment entre le risque, la menace et le danger. La menace et le

danger expliquent la séquence de causalité du risque, car la menace conduit au 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 indésirable dans le sens du "hasard", se différenciant de la menace qui peut être associée au terme "avertissement", car il s'agit d'un indice ou d'un signe laissant prévoir un danger. En ce qui concerne le 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 causes, susceptible de menacer une ou plusieurs cibles".

1.2. Le risque entre danger et opportunité :

Le risque est lié à la prise de décision visant à exposer une cible à un danger. Selon MAZOUNI (2008), le risque représente une potentialité qui se concrétise à travers la réunion de conditions et de circonstances conduisant à l'apparition d'éléments initiateurs. Cela permet ensuite le développement et la propagation de phénomènes, donnant ainsi lieu à l'expression du danger, avec des effets qui affectent un ou plusieurs éléments vulnérables.

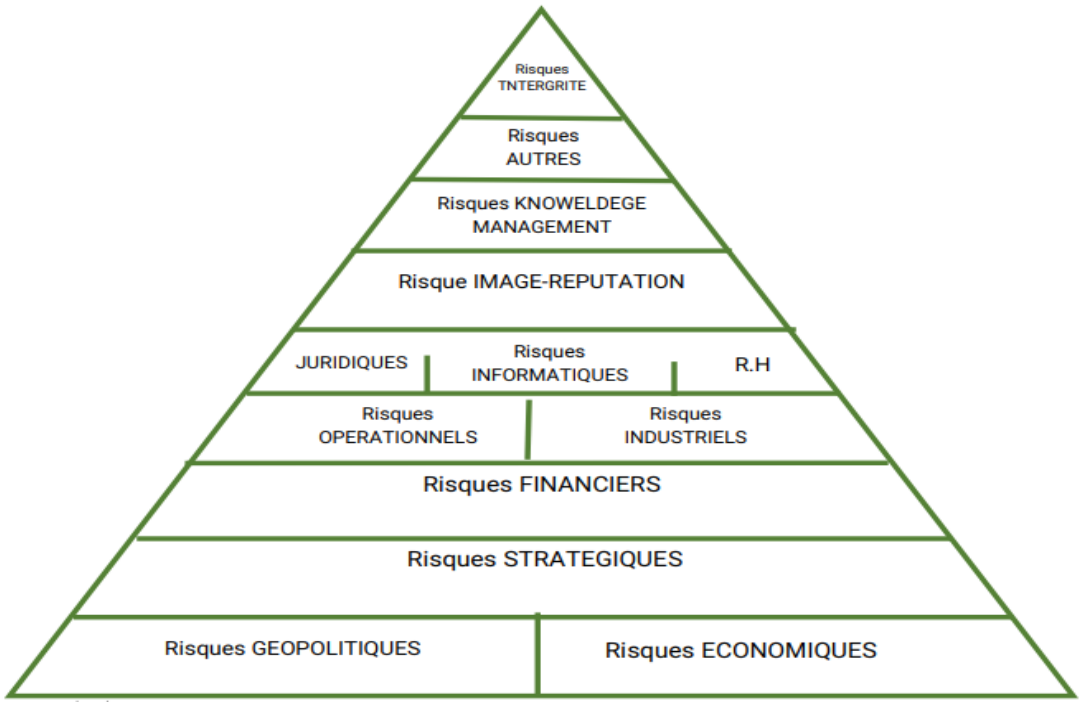
Cependant, le risque n'est pas nécessairement associé à la survenue d'un événement malheureux ou d'un danger. Il peut également être une opportunité pour apprendre et mieux connaître les lacunes de la stratégie d'une entreprise tout en préservant son image de marque, sa qualité de service, et de manière intrinsèque, l'ensemble des enjeux sociaux, économiques, techniques, financiers, juridiques, etc. Le retour d'expérience, selon MAZOUNI (2008), représente une perception intelligente de la notion de risque, consistant à tirer profit de l'occurrence de certains événements indésirables.

1.3.Typologies du risque :

Il existe des centaines de risques qui peuvent compromettre la stabilité des entreprises. Parmi ces risques, treize classes sont particulièrement étudiées en raison de leur impact significatif. Les risques géopolitiques, économiques, stratégiques et financiers occupent les premières positions. Les risques industriels et opérationnels se déclinent en catégories telles que les risques juridiques, informatiques et liés aux ressources humaines.

Les risques d'image et de réputation sont également cruciaux, tout comme ceux associés à la gestion de la connaissance. D'autres risques proviennent de diverses sources, et les risques d'intégrité sont mentionnés en dernier. Darsa a hiérarchisé ces risques dans une pyramide selon un ordre rationnel. En lisant de haut en bas, le risque concerne un individu en haut de la pyramide et le groupe en bas. En sens inverse, la lecture de bas en haut positionne le risque au niveau macroéconomique en bas et au niveau microéconomique en haut.

La figure (04) : représente une pyramide des risques, issue de l'ouvrage "La gestion des risques en entreprise"



Source : de Darsa (2013a), page 72, 3ème édition, publié en France : Gereso.

- **Les risques géopolitiques :** sont fondamentalement liés aux activités internationales des entreprises, impliquent des défis directs ou indirects liés à des pays étrangers. Par exemple, en Russie, le risque est lié à l'exécution souvent faible du droit commercial, tandis qu'au Yémen, l'insécurité et la corruption élevée représentent des menaces, au-delà des zones à risques médiatisées comme l'Irak ou l'Afghanistan.
- **Les risques économiques :** sont associés à l'économie globale dans laquelle l'entreprise opère, incluant des facteurs tels que l'inflation, le PIB et la croissance des marchés. Des risques économiques majeurs peuvent se manifester, comme observé

lors de la crise de 2007-2008, avec l'évolution des cours du pétrole et de ses dérivés, illustrant l'impact sur les entreprises.

- **Les risques stratégiques :** tels que la défaillance d'un modèle stratégique ou une incohérence entre l'analyse des besoins clients et l'offre commerciale, exigent une gestion minutieuse. Par exemple, une croissance externe mal maîtrisée ou une rupture technologique mal anticipée sont des illustrations de risques stratégiques.

- **Les risques financiers :** englobent divers aspects tels que la liquidité, la perte financière, les taux d'intérêt, les taux de change, les marchés financiers, la comptabilité, la fiscalité, la prise de contrôle, les fournisseurs, le sous-investissement, la délinquance financière, l'opportunité de délocalisation, l'arrêt d'activité, la structure des coûts, le haut de bilan, les erreurs d'investissement et le départ des actionnaires.
- **Les risques opérationnels :** résultent de défauts attribuables à des processus internes, des personnels ou des événements extérieurs, pouvant entraîner des pertes dans les cycles d'exploitation quotidiens de l'entreprise.
- **Les risques industriels** : sont spécifiquement liés à la mise en œuvre de processus industriels de production, tels que la perte de qualité, les ruptures de chaîne ou les risques environnementaux.
- **Les risques juridiques** : traités différemment en fonction de leur gravité, concernent les impacts financiers directs ou indirects résultant de l'utilisation inappropriée d'éléments contractuels ou relationnels dans le cadre des activités économiques de l'entreprise.
- **Les risques informatiques** : représentent une catégorie majeure de risques opérationnels, englobant les pertes liées à la défaillance d'éléments matériels, physiques ou logiques constituant l'architecture, les outils, les données ou les applications informatiques de l'entreprise.
- **Les risques liés aux ressources humaines :** comprennent principalement les risques sociaux (climat social, gestion des compétences, etc.) et les risques psychosociaux (mal-être, stress, suicide, etc.), constituant la dernière famille des risques opérationnels traités différemment.
- **Les risques d'image et de réputation :** concernent les dommages économiques significatifs résultant de la détérioration de l'image ou de la réputation de l'entreprise.

- **Les risques de gestion de la connaissance :** également appelés risques de « Knowledge management », visent à renforcer la pérennité d'un actif essentiel de l'entreprise : ses connaissances et ses compétences.
- **D'autres risques** tels que les risques de sur-qualité, de défaillance du contrôle interne, les risques environnementaux, et bien d'autres, sont également présents et variés.
- **les risques d'intégrité :** selon Darsa, occupent le sommet de la pyramide des risques, car l'intégrité individuelle constitue le risque ultime susceptible de compromettre la pérennité de l'entreprise.

1.4. Propriétés du risque :

La gestion des risques en entreprise implique l'application de règles internes, constituant la gouvernance, qui s'imposent aux collaborateurs et décrivent les processus liés aux risques. Cette gouvernance doit être alignée sur la stratégie globale de l'entreprise et refléter sa politique de risque. Élaborées par les directions des risques et adoptées par l'organe d'administration, ces règles doivent être courtes, simples, lisibles et largement diffusées pour assurer la maîtrise complète des risques au sein de l'entreprise.

1.4.1. La culture du risque :

L'intégration de la gestion des risques au niveau opérationnel constitue un élément essentiel, favorisant une approche globale au sein de l'entreprise. Il souligne l'importance de ne pas confiner la gestion des risques à des équipes isolées, mais plutôt de partager la culture du risque avec l'ensemble des acteurs de l'entreprise pour une efficacité optimale du dispositif de gestion des risques.

1.4.2. Le cycle du risque :

Le processus de gestion des risques comporte quatre étapes majeures, selon Dumora (2017):

- La politique de risque : Cette première phase implique la définition et la mise en place de la politique de risque. Elle explique la stratégie et la gestion des risques, ainsi que les processus de décision.
- **La prise de risque :** Cette étape englobe la souscription d'affaires, l'acquisition de portefeuilles ou de compagnies, mais également l'investissement dans des actifs financiers en relation avec les 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, tels que la réassurance, la titrisation, les swaps de portefeuilles, etc.

1.4.3. Cout du risque :

Quel que soit le modèle de gestion des risques choisi, l'objectif principal est de les maîtriser et de faciliter leur classification et leur analyse globale des pertes. Selon Louisot (2005), le coût du risque est la principale motivation pour la gestion des risques. Ce coût comprend cinq éléments : les coûts administratifs liés à la gestion des risques, les coûts des efforts de réduction des risques, les coûts des instruments financiers de transfert des risques, les coûts des rétentions et les coûts des investissements abandonnés dépassant le seuil d'acceptabilité des risques pour l'entreprise.

1.4.4. Appétit au risque :

Le conseil d'administration établit ce qu'on nomme l'"appétence au risque", que la direction adopte en instaurant des contrôles adaptés pour limiter ce risque. L'appétit au risque représente le niveau maximum de risque que l'entreprise est prête à tolérer et à prendre afin d'améliorer sa rentabilité et d'atteindre ses objectifs stratégiques (Brosse et Pets, 2016).

2. La notion du risque opérationnel :

Situés au cœur de la pyramide des risques, les risques opérationnels sont généralement liés à toutes les opérations réalisées par une entreprise, rendant la notion de risque opérationnel extrêmement vaste. Le Comité de Bâle II (2004) a introduit cette notion en tant qu'ensemble de règles pour définir le niveau obligatoire de fonds propres sur les risques. Ces risques opérationnels incluent les pertes provenant de processus internes défaillants, de personnes et systèmes, ou d'événements externes inadéquats. En Algérie, la définition du risque opérationnel est donnée par la réglementation n°2011-08 du 28 novembre 2011, le reliant à des défaillances imputables à des procédures, personnes et systèmes internes, ou à des événements externes. Darsa (2013b) lie les risques opérationnels à l'activité d'exploitation d'une entreprise, provenant des différents processus liés à la mise en œuvre d'un cycle d'exploitation. En général, le risque opérationnel résulte des défaillances des processus, du personnel, des événements et systèmes internes/externes de l'entreprise, entrant dans son activité. Ce risque peut engendrer des dommages et des coûts financiers plus ou moins graves,

avec un impact interne sur le cycle d'exploitation et un impact externe lié à la satisfaction du client, nécessitant une couverture importante.

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 en fonction des défaillances qu'ils engendrent. Ces sous-ensembles comprennent les défaillances liées au système d'information, aux processus, aux personnes et aux événements extérieurs.

Défaillance liée au système d'information : Ce risque est associé aux faiblesses du niveau de sécurité des systèmes informatiques, pouvant entraîner des pannes matérielles, des interruptions d'activité et des risques comptables liés à des informations erronées.

Défaillance liée aux processus : Cette défaillance englobe les risques liés au non-respect des procédures, à une mauvaise gestion des processus, à l'interruption d'activité, à l'interruption des systèmes, au risque comptable et au risque de blanchiment.

Défaillance due aux personnes : Générée par le risque lié aux processus, elle dépend de la qualité du personnel et inclut les sous-risques de fraude, déontologique et de mauvaise gestion du personnel.

Défaillance due aux événements extérieurs : Ce risque est lié à des événements externes tels que des risques politiques ou des catastrophes naturelles. Il comprend des sous-risques tels que le risque juridique, réglementaire, sur clients, produits et pratiques commerciales, ainsi que le risque de dommages liés aux actifs corporels résultant de catastrophes naturelles.

2.2.Enjeux liés aux risques opérationnels :

Darsa (2013b) souligne l'importance de comprendre et maîtriser les cycles d'activités d'une entreprise avant de mettre en évidence les risques opérationnels fondamentaux. Ces cycles se répartissent en quatre grandes familles : infrastructure, exploitation, commerciale et support, chacune ayant ses propres enjeux liés aux risques.

- **Infrastructure :** Veiller à la pérennité des actifs de l'entreprise est crucial pour assurer la continuité des services et la satisfaction du client. Les enjeux incluent l'accès, la

sécurité des produits et services, ainsi que la sécurisation des actifs logiques et virtuels.

- **Exploitation :** L'identification des risques liés au cycle d'exploitation révèle la complexité des enjeux organisationnels. Des cycles tels que l'approvisionnement, les achats de matières premières, et la production présentent des défis liés à la continuité, à la qualité et à la maîtrise des risques.
- **Commerciale :** Les cycles commerciaux sont sources de risques opérationnels liés directement au client. Les enjeux comprennent la gestion des relations clients, la fidélisation et la gestion des risques pour assurer une production continue de qualité.
- **Support :** Les processus de support, tels que l'administration interne, doivent sécuriser leurs mécanismes pour éviter des impacts directs ou indirects sur le client. Les enjeux qualité et gestion de la connaissance sont également cruciaux.

En plus de ces familles, les enjeux du risque opérationnel s'étendent à d'autres dimensions telles que la sous-traitance, la fraude interne et externe, la conformité des opérations, les risques informatiques, juridiques et humains. Cela montre que tout peut être considéré comme un risque opérationnel, obligeant les organisations à définir clairement ce qui sera considéré comme tel au-delà des enjeux.

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

La démarche d'inventaire des risques opérationnels selon Darsa (2013b) consiste en plusieurs étapes :

- **Collecte de signaux précurseurs :** Identification des signaux annonciateurs de risques opérationnels, tels que réclamations, plaintes, remarques négatives de tiers, clients, fournisseurs ou employés.
- **Audit interne et externe :** Inspection des locaux de l'entreprise et visites chez les fournisseurs et clients pour recueillir des informations.
- **Collecte des incidents et dysfonctionnements :** Identification des incidents et dysfonctionnements ayant entraîné des coûts liés aux risques, comme les pertes liées à une mauvaise gestion ou à une perception négative par un client.
- **Cartographie des processus opérationnels :** Élaboration d'une cartographie des processus par service, processus et sous-processus, incluant les modes opératoires et schémas des flux.

- **Qualification du niveau de criticité :** Évaluation du niveau de criticité des processus et sous-processus de l'entreprise en maîtrisant les risques opérationnels présents.

Une fois cet inventaire réalisé, l'entreprise est confrontée à une multitude de risques qui, dans un premier temps, peuvent tous être considérés comme des risques opérationnels. Pour définir ce qui est opérationnel ou non, elle doit déterminer le degré de mesure de l'enjeu pour chaque risque, afin de délimiter le champ des risques opérationnels en écartant ceux qui ne le sont pas. Cette délimitation des enjeux permet également de réduire le coût des risques opérationnels dans l'entreprise. Ensuite, une fois la notion de risque opérationnel maîtrisée, l'étude des différentes composantes et typologies de ce risque peut être approfondie.

2.3.Typologie du risque opérationnel :

En 1999, Thain Nguyen Hong a été le premier à réaliser une classification des risques opérationnels en deux typologies, à savoir les risques de dysfonctionnement et les risques de manipulation frauduleuse (Raïs H.M, 2012). Bâle II a classé les risques opérationnels en sept catégories : la fraude interne, la fraude externe, l'insuffisance des pratiques internes concernant les ressources humaines et la sécurité du lieu de travail, les clients, les produits et les pratiques commerciales (manquement, délibéré ou non, à une obligation professionnelle envers un client, à la nature ou aux caractéristiques d'un produit), les dommages aux actifs physiques, l'interruption d'activité et le dysfonctionnement des systèmes, le dysfonctionnement des processus de traitement-exécution (passation d'ordre, livraison), et la gestion des processus intégrant les relations avec les contreparties commerciales et les fournisseurs. (Caclin F, 2021)

Un groupe de travail de l'IFACI, l'Institut Français d'Audit et de Contrôle Internes, a élaboré une nomenclature des risques pour les entreprises d'assurance. Le référentiel proposé est constitué de trois niveaux : 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 al. 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 enchaînement de différentes natures.

2.3.1. Les sept catégories de RO :

L'Institut des Actuaires Français (IA) a élaboré une typologie du risque opérationnel articulée en trois niveaux. Le premier niveau aligne ses catégories sur les 7 définies par Bâle 3, facilitant ainsi un regroupement équivalent des risques. Le deuxième niveau propose des catégories plus détaillées, mettant en lumière des spécificités propres au secteur de l'assurance. Enfin, le dernier niveau présente une liste non exhaustive d'exemples de risques, offrant ainsi une vision détaillée et classifiée des différentes formes de risques opérationnels.

Tableau(4) : Classement des risques opérationnels inspiré de «Le risque opérationnel, un nouveau challenge pour l'actuaire»

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.

Source : Institut des Actuaires. (2016) ; p 15 https://www.institutdesactuaires.com/global/gene/link.php?doc_id=9761&fg=1

2.3.2. Les risques juridiques :

La question du risque juridique, souvent négligée et sous-traitée par les dirigeants, a gagné en importance en raison de sa diversité et de son impact potentiellement négatif sur l'organisation. Un risque juridique se définit comme une menace financière directe ou indirecte pour l'entreprise, découlant d'une utilisation inappropriée ou d'une application défectueuse d'éléments contractuels ou relationnels dans le cadre de ses activités économiques, pouvant être régis par la doctrine juridique ou les us et coutumes en vigueur (Darsa, 2013b, p.148). Les multiples causes de ces risques peuvent être contractuelles, telles que la qualité et l'intégrité des contrats clients, fournisseurs, distributeurs, de franchise, de prestations critiques et externalisées, ainsi que des contrats d'assurance, de baux (locaux) et de travail. Au niveau de la conformité des processus opérationnels avec la loi, les principales sources de risques juridiques concernent le respect ou la maîtrise du droit du consommateur, commercial, de la concurrence, du droit pénal et des marques, ainsi que la conformité aux codes de la propriété intellectuelle, monétaire et financier, du travail, des marchés publics, et la législation comptable, financière, fiscale et sociale. Un autre aspect à ne pas négliger concerne les risques liés aux contentieux, englobant les litiges commerciaux ou techniques, les comportements commerciaux inadaptés, les situations d'insolvabilité, les défaillances financières des débiteurs et les processus d'identification insuffisants des risques clients.

- Dans un contexte où la pénalisation du monde des affaires est en croissance, un risque juridique particulièrement préoccupant concerne les infractions pénales. Les dirigeants et l'entreprise encourent des risques s'ils ne parviennent pas à identifier et maîtriser ces infractions. Parmi les infractions pénales courantes figurent l'abus de confiance, la contrefaçon de logiciels, le financement du terrorisme, etc. La vigilance et une gestion adéquate de ces risques sont essentielles pour éviter les conséquences néfastes sur les dirigeants et l'entreprise dans son ensemble.

2.3.3. le risque informatique :

La maîtrise du risque informatique revêt une importance capitale dans la stratégie d'une entreprise, bien plus que la négligence du risque juridique. Cette préoccupation est essentielle pour garantir la pérennité opérationnelle de l'organisation et contenir les coûts associés. Le risque informatique, également connu sous le nom de risque des technologies de l'information et de la communication (TIC), correspond au risque de subir des pertes résultant d'une

organisation inadéquate, d'un dysfonctionnement ou d'une sécurité insuffisante du système d'information. Ce dernier englobe l'ensemble des équipements, des systèmes, des réseaux et des ressources humaines dédiés au traitement de l'information au sein de l'institution. Une gestion efficace de ce risque est cruciale pour préserver la stabilité opérationnelle de l'entreprise.

2.3.3.1. Causes, conséquences et impacte financier :

La survenance d'un risque informatique peut entraîner des coûts financiers variables, dépendant de la gravité et de la complexité de la gestion du risque. Ces coûts peuvent se manifester par une perte de productivité et/ou des frais de remplacement, impactant l'image auprès des clients et fournisseurs, ainsi que la fiabilité des outils informatiques. Les conséquences incluent l'indisponibilité temporaire ou permanente d'applications, de serveurs, de réseaux ou de matériel comme les serveurs web, engendrant des pertes d'exploitation et handicapant opérationnellement les équipes techniques privées d'outils. Les causes de ces risques comprennent les pannes d'infrastructures, de matériels ou de logiciels, les attaques virales, les violations de la sécurité physique (vol, incendie) et le potentiel insuffisant des machines.

2.3.3.2. Appréhension du risque informatique :

En tant que risque majeur, technique et source d'innovation et de différenciation de valeurs pour l'entreprise, la gestion rapide, efficace et mise à jour du risque informatique est cruciale. Diverses approches d'identification sont proposées, chacune offrant une pertinence différente et présentée sous forme de check-lists d'enjeux et de points à considérer (Darsa, 2013b) :

- **L'approche générale :** offre une première liste de risques à considérer, orientée vers les grands axes fonctionnels et organisationnels de l'entreprise.
- **L'approche « menaces »** : permet d'identifier les risques liés à l'infrastructure informatique, comportant 18 points spécifiques.
- **L'approche synthétique :** complémentaire de la précédente, contient une liste de 27 risques informatiques présents dans chaque entreprise.
- **L'approche IT (informatique) :** constitue une liste exhaustive de 99 enjeux liés à la maîtrise opérationnelle du risque informatique.

- **L'approche projet ou « risque projet » :** souligne que la non-maîtrise d'un projet informatique engendre divers risques informatiques. Une liste de 79 risques projet est proposée pour amorcer tout projet informatique.

2.3.4. Risques sociaux et psychosociaux :

- **Risques sociaux :**

Les risques sociaux comprennent également une dimension particulière, le risque psychosocial, qui relève de l'individu lui-même, indépendamment de sa fonction ou de son positionnement dans l'entreprise (Darsa, 2013b). Les risques psychosociaux comprennent divers aspects tels que le stress, le mal-être, les conduites suicidaires, les agressions physiques ou verbales entre collaborateurs et responsables, ainsi que le risque d'enlèvement, de séquestration ou d'assassinat de collaborateurs ou de dirigeants. En raison de leur variété, il peut être difficile pour les encadrants de les identifier et de les appréhender. Face à ces risques, la communication joue un rôle essentiel, impliquant l'échange avec les salariés et les encadrants, l'écoute de leurs plaintes et réclamations, et le refus d'accepter des situations intolérables (Darsa, 2013b).

- **Risques psychosociaux :**

Le risque psychosocial, distinct du risque social général, concerne l'individu au sein de l'entreprise. Les risques associés incluent le stress, le mal-être, les conduites suicidaires, les agressions entre collaborateurs, ainsi que les risques d'enlèvement ou d'assassinat. Identifier et comprendre ces risques variés peut être complexe pour les encadrants. La communication joue un rôle crucial, impliquant l'échange avec les salariés, l'écoute de leurs préoccupations, et le refus de tolérer des situations intolérables (Darsa, 2013b).

2.4. Facteurs de développements des RO :

L'évolution récente de la perception du risque opérationnel s'explique par son importance croissante, résultant de divers facteurs majeurs qui ont contribué à son développement au fil du temps.

2.4.1. Fonctionnement des marchés :

La globalisation des marchés et des produits a intensifié la concurrence entre les établissements, élargissant leurs domaines d'intervention et augmentant les risques associés. Les évolutions technologiques, notamment la gestion en temps réel, ont donné naissance à de nouveaux risques tels que le règlement, la fraude interne ou externe, et les défaillances techniques et humaines.

2.4.2. Sophistication des techniques financières :

Les nouvelles techniques financières complexes rendent la gestion des risques plus difficile. Le développement du commerce électronique soulève des questions de fraude et de sécurité informatique, tandis que les montages financiers élaborés exposent les établissements à un risque juridique accru.

2.4.3. Évolution des processus internes :

L'automatisation croissante des processus internes grâce aux outils informatiques génère des risques techniques. Le recours à l'externalisation de certaines activités contribue également à l'accroissement des risques opérationnels.

2.4.4. Événements extérieurs :

Les risques exceptionnels, tels que les catastrophes naturelles, bien que rares, suscitent une attention accrue en raison de leur forte intensité. Ces événements extérieurs présentent des risques importants malgré leur faible occurrence.

3. Organisation du contrôle du RO :

La gestion des risques opérationnels au sein de l'entreprise implique une multitude d'acteurs répartis à tous les niveaux et dans toutes les fonctions. En période de crise, ces acteurs doivent collaborer efficacement pour optimiser la création de valeur. Pour atteindre cet objectif, il est crucial de définir clairement les responsabilités, missions et interactions des acteurs, tout en fixant des objectifs précis. Une politique de maîtrise des risques opérationnels efficace nécessite l'engagement transparent des dirigeants à tous les niveaux de l'entreprise. Une organisation efficiente repose sur la définition précise des responsabilités pour chaque fonction. Pour garantir la pérennité de l'entreprise, sécuriser les activités et protéger le

patrimoine, il est essentiel que chaque membre contribue à limiter et anticiper les risques, favorisant ainsi une culture proactive de gestion des risques (Merlier et Jimenez, 2004).

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

Selon Merlier et Jimenez (2004), la direction générale joue un rôle crucial dans la mise en place d'un dispositif de gestion des risques opérationnels. Elle est responsable de la politique de risque, des allocations de couverture, et assure la réalité et l'efficacité du dispositif devant les autorités de contrôle. La direction générale assume quatre responsabilités essentielles, notamment la mise en œuvre du système de gestion et de maîtrise des risques, la stratégie de couverture des risques opérationnels et l'acceptation des risques résiduels, l'allocation des fonds propres nécessaires à la couverture des risques, et enfin, la garantie d'un audit régulier du système de manière indépendante pour vérifier son exhaustivité et sa qualité.

3.2. La direction des RO et les lignes métiers :

Selon Merlier et Jimenez (2004), la direction des risques opérationnels est l'outil principal d'assurance de l'efficacité des processus pour la direction générale. Elle offre une vision transversale qui favorise la prévention plutôt que le traitement ponctuel des risques. Pour atteindre cette efficacité, il est essentiel d'assurer une indépendance des fonctions opérationnelles.

3.2.1. Les missions de la direction des RO :

Merlier et Jimenez (2004) définissent les missions de la direction des risques opérationnels, comprenant la création de politiques et procédures, la coordination des travaux dans les lignes métiers, la validation et mise en œuvre de modèles, la définition d'outils de mesure et suivi, la consolidation des données, l'analyse des remontées d'informations, le contrôle des incidents, l'intervention dans des dossiers à fort impact, et la participation à la validation des états réglementaires.

3.2.2. Les lignes métiers et les opérationnels :

La politique de maîtrise des risques, selon Merlier et Jimenez (2004), implique plusieurs enjeux, dont le plus notable est la formation et la mobilisation des équipes face aux risques

existants et à la gestion des incidents. Le dispositif opérationnel comporte généralement trois niveaux de responsabilités distinctes.

Au premier niveau, la direction de la fonction opérationnelle est chargée de mettre en place la politique des risques, de décider des mesures prioritaires, d'établir des plannings, et de veiller à la formation du personnel et à la mise à jour du dispositif.

Au deuxième niveau, le management met en place des outils d'évaluation et de reporting, valide les informations sur les incidents, les traites, et assure la transparence du dispositif.

Enfin, le troisième niveau concerne les opérationnels qui gèrent les processus et la production, détectent et enregistrent les incidents, mettent en place des mesures correctives et conservatoires, et proposent des plans d'action pour corriger les incidents.

3.3. La relation entre les RO et les lignes transverses :

Les métiers transverses, selon Merlier et Jimenez (2004), sont généralement responsables de risques particuliers et sont soumis à des contraintes spécifiques nécessitant parfois des traitements 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.

3.3.1. Les systèmes d'information :

L'intervention des personnes en charge du système d'information (SI) revêt une importance cruciale lors de la mise en place d'un SI adapté aux besoins des risques opérationnels, contribuant ainsi à leur maîtrise. Généralement, on observe une direction des Systèmes d'Information (DSI) et un Responsable de la Sécurité des Systèmes d'Information (RSSI) qui sont responsables des risques associés au SI.

3.3.2. Les ressources humaines :

Les responsables du système d'information ont un rôle crucial dans l'identification des risques liés aux collaborateurs de l'entreprise, qu'ils soient individuels ou collectifs. L'intégration d'événements ponctuels est essentielle dans la mesure des risques opérationnels. Certains risques, comme les accidents de travail, les fraudes ou les vols, nécessitent une protection des données nominatives et une limitation de l'accès aux personnes autorisées. Les risques liés

aux ressources humaines incluent l'inadéquation des compétences, le turnover des équipes et la sensibilité des personnes pour une activité donnée. (Merlier et Jimenez, 2004).

3.3.3. La logistique :

Les responsabilités liées à la sécurité des biens et des personnes sont généralement confiées à des individus spécialisés possédant des compétences en gestion immobilière, sécurité incendie, gestion des accès, négociations avec les fournisseurs, etc. En cas de décentralisation de ces fonctions au sein des métiers opérationnels, le schéma traditionnel, tel que

Précédemment exposé, sera maintenu. Il est recommandé, dans ce contexte, de sensibiliser particulièrement les personnes en charge de ces domaines (Merlier et Jimenez, 2004).

3.3.4. Les services juridiques :

Les services responsables des risques spécifiques sont bien formés et jouent un rôle préventif important, ils ne sont pas enclins à dissimuler des informations pouvant compromettre leur responsabilité, car ils ne sont pas à l'origine des dossiers contentieux. La relation avec le suivi des risques opérationnels se déroule naturellement et ne pose généralement pas de problèmes particuliers, selon 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 cruciale pour garantir la réalité et la matérialité du système de contrôle interne. À travers des inspections régulières, elle contrôle la mise en œuvre des politiques de sécurité, de respect des règles internes et de la réglementation définie par la direction générale. Cette fonction doit maintenir une totale indépendance pour assurer son objectivité et ne pas être impliquée dans la définition et la mise en œuvre des politiques et outils de maîtrise des risques opérationnels. Son rôle principal est de valider la pertinence et la qualité du système de maîtrise des risques et de proposer des mesures d'amélioration.

3.4.1. Le RO et le contrôle interne :

La mise en place des mesures de contrôle interne vise à assurer la maîtrise des risques au sein de l'entreprise, grâce à un processus de gestion des risques opérationnels intégré. Cela inclut divers éléments tels que le contrôle des opérations, les procédures internes, l'organisation comptable, les systèmes de mesure des risques et des résultats, la surveillance et la maîtrise

des risques, la documentation et le traitement de l'information, ainsi que la surveillance des flux d'espèces et de titres (Merlier et Jimenez, 2004). Le dispositif de maîtrise des risques opérationnels complète ces principes en permettant la mesure de risques jusqu'alors peu appréhendés, intégrant ainsi les risques opérationnels dans la démarche globale de contrôle interne.

SECTION 3 : LA GESTION DES RISQUES DES SYSTEMES D'INFORMATION

L'approche actuelle de la sécurité des systèmes d'information se base sur la gestion des risques, visant à réduire significativement les pertes résultant des vulnérabilités de ces systèmes. L'évolution du métier de Risk Manager, axé sur la sécurité du système d'information, permet une meilleure appréhension et gestion des risques informatiques.

1. La fonction gestion des risques d'un SI :

La gestion des risques, telle que définie par l'ISO/IEC dans le Guide 73 (2009), consiste en un ensemble d'activités coordonnées visant à guider et superviser un organisme face aux risques. Ses objectifs incluent l'amélioration de la sécurité des systèmes d'information, la justification des budgets dédiés à la sécurité, et la démonstration de la crédibilité du système par le biais d'analyses approfondies. L'objectif premier de la gestion des risques pour un système d'information est d'assurer sa sécurité en adaptant les méthodes de gestion en fonction des risques estimés.

Cette démarche s'appuie sur un comité appelé Team Risk Management (TRM), chargé d'identifier et d'évaluer les risques afin de déterminer les meilleures réponses possibles. Le TRM oriente son approche autour de quatre catégories de risques : le risque stratégique, le risque opérationnel, le risque lié aux projets et le risque de litige (Guide 73:2009).

1.1. Avantages de la gestion des risques SI :

La gestion du risque lié aux systèmes d'information (SI) offre plusieurs avantages :

- **Prise de décisions rationnelles :** La gestion du risque pour les systèmes d'information aide les organisations à prendre des décisions éclairées en matière de sécurité.
- **Gouvernance du risque du SI :** Protège la technologie et l'infrastructure physique des systèmes, favorisant ainsi la croissance de l'activité et la création de valeur.

- **Prévention des détériorations et utilisations anormales :** Vise à prévenir les atteintes aux systèmes et réseaux, assurant ainsi leur intégrité et disponibilité.
- **Détection des atteintes à la confidentialité :** La gestion des risques permet de détecter et de limiter les conséquences des atteintes à l'intégrité, la disponibilité et la confidentialité des informations.
- **Avantages selon Westerman et Hunter :** Une approche efficace, intégrant gouvernance, assise informatique, et culture de prise en compte des risques, conduit à une meilleure performance opérationnelle.
- **Réponse aux insuffisances :** La gestion du risque permet de faire face aux sensibilisations insuffisantes et aux lacunes en personnel formé ou en outils.
- **Meilleures performances informatiques :** Elle contribue à améliorer la prévention des incidents, accompagner l'évolution de l'entreprise, et aligner les objectifs informatiques et métier.
- **Évitement des risques financiers :** La gestion du risque permet d'éviter des conséquences financières telles que la perte de réputation, la réduction de la valeur des actions, et la perte de compétitivité.

1.2. Le top 10 des risques opérationnels lié aux SI :

En 2015, l'Institute of Internal Auditors (IIA) a réalisé une étude appelée CBOK (Common Body of Knowledge) visant à identifier les dix principaux risques liés aux systèmes d'information (SI). Cette analyse a été menée à travers des entretiens avec des responsables de l'audit interne et des experts en SI à l'échelle mondiale. Il est important de noter que l'ordre de priorité de ces risques peut varier en fonction du secteur d'activité.

1.2.1. Cybersécurité :

Le vol d'informations sensibles par intrusion est identifié par 82% des experts en systèmes d'information comme le risque le plus significatif. Cette préoccupation est partagée par les dirigeants, les auditeurs internes et les administrateurs en raison des conséquences graves qu'une telle fuite de données pourrait avoir sur l'image de marque et la réputation de l'entreprise.

1.2.2. Protection des données :

Historiquement, la préservation des données, en ce qui concerne leur confidentialité, intégrité et accès, reposait sur des dispositifs tels que les pare-feux, les systèmes de prévention et de détection des intrusions, les outils de filtrage des contenus, ainsi que les mécanismes de surveillance du réseau. Cependant, cette approche mono-niveau s'est avérée inefficace. Ainsi, une nouvelle orientation privilégie désormais une stratégie de protection multi-niveaux, sous la direction du responsable de la sécurité des systèmes d'information, englobant 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 mesures strictes en matière de sécurité physique.

1.2.3. Les projets SI :

Chaque organisation ressent la nécessité de moderniser ses systèmes d'information, principalement en raison des coûts élevés associés aux défaillances logicielles. Afin de répondre à cette exigence, des budgets conséquents sont alloués aux projets informatiques. Malheureusement, la réussite de ces initiatives est souvent compromise, les risques inhérents incluant :

- Non-respect des délais et du budget.
- Défaillance des logiciels en raison d'une insuffisance de tests préalables au déploiement.
- Réduction de l'efficacité et de l'intégration par rapport au plan initial.
- Fonctionnalités inférieures par rapport aux projections initiales énoncées dans le business case du projet.

- Le défaut de leadership représente un problème significatif, pouvant avoir des répercussions sur le projet à divers niveaux, en particulier en ce qui concerne la gestion des risques.

1.2.4. Gouvernance des SI :

La gouvernance des systèmes d'information (SI), englobant la direction, les structures organisationnelles et les processus, a pour objectif de garantir que les technologies de l'information soutiennent efficacement la stratégie et les objectifs de l'organisation (IIA/IFACI 2013). Face aux investissements importants dans les SI et à leurs répercussions sur les clients et les opérations, la gouvernance des SI doit assurer la performance de ces systèmes en maîtrisant les risques et en saisissant les opportunités d'amélioration.

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

- S'aligner clairement sur les besoins métiers.
- Générer une valeur mesurable pour les métiers.
- Intégrer des mécanismes de contrôle et de reddition de comptes concernant les ressources, les risques, les performances et les coûts.

1.2.5. Prestation informatique externalisé :

L'externalisation comporte des risques potentiels pour une organisation, souvent méconnus jusqu'à ce qu'une défaillance survienne. Afin de les prévenir, les responsables doivent veiller à ce que le contrat initial englobe des aspects tels que la supervision, la surveillance, l'audit, la sécurité physique et logique, la dotation en personnel appropriée, la désignation d'un interlocuteur clé, l'accès à l'information, les plans de continuité d'activité/reprise après sinistre, les contrats de niveau de service, et le reporting.

1.2.6. Utilisation des réseaux sociaux :

La propagation rapide des communications sur les réseaux sociaux a obligé les organisations à établir des règles pour éviter les risques juridiques, de fuites d'informations sensibles et de dommages à la réputation. Pour contrer ces risques, elles doivent mettre en place une politique d'utilisation des réseaux sociaux, surveiller son application et sanctionner les violations.

1.2.7. Informatique mobile :

Les données mobiles doivent bénéficier de mesures de sécurité aussi robustes que celles des sièges des organisations, car l'information se déplace avec l'utilisateur. La disponibilité généralisée de la connectivité Internet et la puissance informatique actuelle ont entraîné l'émergence de nombreux risques liés aux divers dispositifs et configurations réseau. Cette situation remet en question les approches traditionnelles de gestion des risques par les DSI.

- **Risques liés à la sécurité :** La perte ou le vol d'appareils contenant des données personnelles ou sensibles de l'organisation peut compromettre la sécurité, en particulier si les dispositifs de contrôle de sécurité ne sont pas efficaces.

- **Risques liés à la conformité :** Avec l'introduction de la politique BYOD, les organisations dépendent largement des utilisateurs pour respecter les règles et procédures, mais celles-ci peuvent être contournées, notamment en raison de la fréquence élevée des mises à jour.

- **Risques liés à la protection de la vie privée :** La politique BYOD peut soulever des inquiétudes concernant la protection de la vie privée, tant du point de vue de l'organisation que des collaborateurs.

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

- **Risques juridiques :** Les conséquences juridiques liées au stockage de données de l'organisation sur des appareils intelligents doivent être prises en considération pour éviter d'éventuelles implications juridiques néfastes.

1.2.8. Compétences des auditeurs internes en matière de SI :

Mark Salamasick, directeur du département Audit de l'Université du Texas, explique que le faible nombre d'auditeurs compétents en SI s'explique par plusieurs raisons. La principale est que les professionnels des SI peuvent être attirés par des technologies plus innovantes et demander des rémunérations plus élevées que les auditeurs SI. Certaines organisations

forment en interne leurs auditeurs financiers et opérationnels aux SI, mais ils ne sont pas toujours officiellement accrédités par la DSI et la direction.

1.2.9. Technologies émergentes :

L'évolution des systèmes d'information entraîne l'émergence de nouveaux risques pour les organisations. Les technologies émergentes telles que le big data, l'impression 3D et la robotique peuvent avoir des conséquences diverses selon leur déploiement dans les organisations. Dans le secteur financier, le niveau de risque inhérent associé à la fiabilité du big data est perçu comme étant le plus élevé.

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

Les systèmes d'information sont un élément crucial pour toute organisation, nécessitant un investissement significatif. Il est donc risqué pour le Conseil d'administration de ne pas posséder une expertise suffisante dans ce domaine. Il devrait acquérir les compétences nécessaires pour évaluer précisément la performance des SI auprès du Directeur des Systèmes d'Information (DSI), tout comme il a renforcé ses compétences financières au fil du temps.

1.3.Méthodes de gestion des risques SI :

La complexité associée à la notion de risque, ainsi que la profusion de normes et de modèles dédiés à sa gestion, avec plus de 200 méthodes de gestion et d'analyse des risques disponibles à l'échelle mondiale, rendent difficile pour les organisations le choix de la méthode la plus adaptée à leur activité (Mayer et Humbert, 2006). Une bonne compréhension des fondements de la gestion des risques pour les systèmes d'information serait donc essentielle pour prendre une décision optimale quant à la méthode à adopter.

Selon l'étude de Mayer et Humbert (2006), les méthodes les plus utilisées dans ce domaine ont été identifiées comme suit :

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

Créée en 1995 par la DCSSI, EBIOS est une méthodologie de gestion des risques pour les systèmes d'information. Elle comprend cinq guides et un logiciel support, offrant une approche adaptée au contexte de l'organisation cible en mettant l'accent sur les éléments essentiels du système d'information. EBIOS permet également de déterminer les besoins en

sécurité et de préparer les contre-mesures appropriées en se basant sur les normes ISO 15408, 17799. Certains estiment cependant qu'elle se limite à une analyse des risques sans couvrir toutes les étapes de la gestion des risques.

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

Émanant du Software Engineering Institute (SEI) de la Carnegie Mellon University, reconnue dans le domaine de la sécurité des systèmes d'information (certifiée par la fédération des Computer Emergency Response Team - CERTS), cette méthodologie se distingue par son approche utilisant uniquement les ressources internes de l'organisation pour évaluer les risques sur ses actifs opérationnels. Elle suit un processus en trois phases pour mesurer ces vulnérabilités :

- **La phase 1 :** vue organisationnelle, permet l'identification des ressources informatiques critiques, des menaces qui y sont associées et des exigences de sécurité qui leur sont liées.
- **La phase 2 :** vue technique, permet d'identifier les vulnérabilités de l'infrastructure, ces vulnérabilités combinées aux menaces créant le risque.
- **La phase 3 :** consiste en l'élaboration de la stratégie de sécurité et de son plan d'action, incluant la protection et la réduction des risques.

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

MEHARI, maintenue en France par le CLUSIF, est une méthodologie d'analyse des risques dérivée de MARION et MELISA. Elle permet d'analyser les enjeux de sécurité, d'auditer les services de sécurité, et d'évaluer les situations de risque. Elle est applicable à la fois au niveau stratégique et opérationnel, assurant la cohérence des besoins organisationnels et définissant les unités business autonomes. En se basant sur l'audit de sécurité, MEHARI facilite l'élaboration de plans d'actions pour remédier aux faiblesses identifiées, ainsi que la gestion des risques de projets en intégrant un plan d'action directement au projet. MEHARI est alignée avec les deux premières méthodes en termes de couverture du processus de gestion des risques.

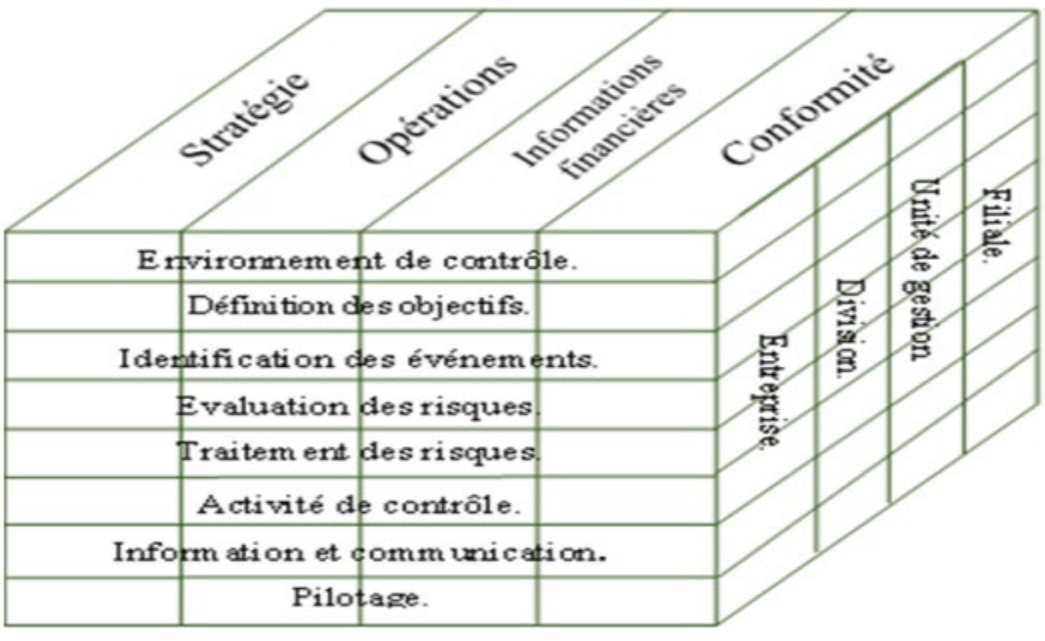
2. Référentiels normatifs liés à la gestion des risques SI :

Dans le domaine du management des risques, l'utilisation de référentiels est indispensable pour standardiser les pratiques, notamment en ce qui concerne les processus de gestion des risques. Parmi les référentiels les plus anciens, on trouve l'Australian/New Zealand Standard 4360, approuvé par l'ISO, qui met l'accent sur l'intégration de la culture du risque dans l'organisation (Dale F. Cooper, 2007). D'autres référentiels notables incluent le modèle Criteria on Control Committee (COCO) au Canada et le Turnbull guidance au Royaume-Uni. Le référentiel européen Fédération of European Risk Management (FERMA) regroupe les meilleures pratiques européennes en gestion des risques. Dans ce contexte, nous mettrons en avant les référentiels les plus couramment utilisés.

2.1. COSO et COSO-ERM :

Le COSO (Committee of Sponsoring Organizations) est un cadre de gestion des risques en entreprise créé en 1985 pour lutter contre la fraude et la corruption. Il vise à renforcer la gouvernance d'entreprise. Son premier document a été publié en 1992, suivi par COSO2 en 2004, et une mise à jour en 2013 pour répondre aux nouveaux environnements opérationnels et aux attentes accrues en matière de contrôle interne. Le COSO définit le management des risques comme un processus impliquant toute l'organisation, visant à identifier et gérer les risques dans les limites de son appétence pour le risque. Il fournit une orientation claire pour la gestion des risques d'entreprise en définissant les composants essentiels et en suggérant un langage commun, représentés dans une matrice à trois dimensions.

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



Source : IFACI, 2017, p.5.

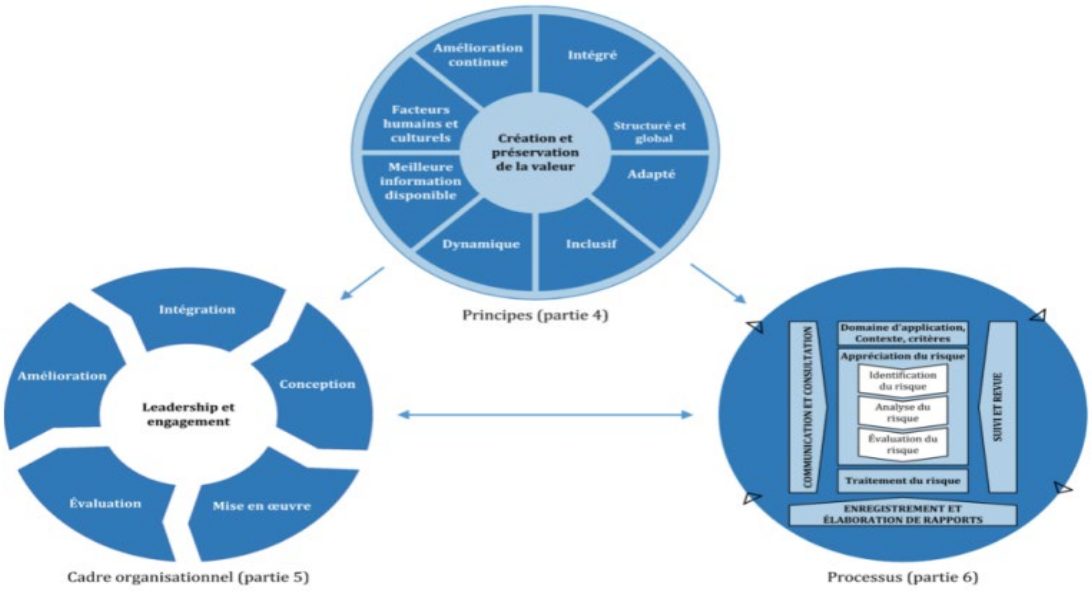
2.2.CobiT (Control Objectives for Information and Related Technology) :

Le CobiT, publié en 1996, est une méthodologie d'évaluation des services informatiques et de gouvernance IT. Il propose un ensemble de bonnes pratiques couvrant divers domaines fonctionnels, tels que la planification, l'acquisition, la distribution et la surveillance des services informatiques. Avec 34 processus couvrant 318 objectifs, le CobiT permet d'aligner les systèmes d'information sur les besoins métier, d'apporter une valeur ajoutée aux métiers, et de gérer efficacement les ressources et les risques. Il est essentiel pour une bonne gouvernance d'entreprise, en particulier en abordant la gouvernance de la sécurité de l'information avec des processus comme la prise de conscience du management, l'évaluation et la gestion des risques, l'assurance d'un service continu et la sécurité des systèmes.

2.3. La norme ISO 31000 (Management Du Risque) :

Modifiée en 2018, la norme internationale ISO 31000 pour le management des risques est élaborée par le comité technique ISO/TC262 de l'Organisation internationale de normalisation (ISO). Cette norme s'adresse à tous les types d'organismes, quelle que soit leur taille, leur activité ou leur emplacement, et fournit des principes et des lignes directrices générales pour le management des risques. Son processus est applicable à toute organisation souhaitant augmenter ses chances d'atteindre ses objectifs, identifier les opportunités et les menaces, et allouer efficacement les ressources pour le management du risque. Elle rappelle que l'intérêt du management des risques réside dans son application à tous les domaines de l'organisation. L'ISO 31000 aide les organismes à développer une stratégie de management du risque efficace, favorisant l'atteinte des objectifs et la protection des actifs. Son objectif premier est de contribuer au développement d'une culture du management des risques, sensibilisant les

employés et les parties prenantes à son importance. La mise en œuvre de l'ISO 31000 permet également aux organismes de comprendre les opportunités et les conséquences associées aux risques, les aidants à prendre des décisions plus éclairées et efficaces, notamment en matière d'affectation des ressources. Cette norme joue un rôle essentiel dans l'amélioration de la gouvernance d'un organisme et, à terme, de sa performance.



Figure(06) : Principes, cadre organisationnel et processus de la norme ISO 31000.

Source : 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 Informatiques et/ou d'Information (DSI) joue un rôle central dans la stratégie informatique de l'entreprise. Historiquement technique, son rôle a évolué vers une contribution essentielle à la formulation des objectifs stratégiques, grâce à l'essor de la gestion des données électroniques. Les DSI sensibilisent les cadres dirigeants et les employés aux avantages et aux risques des systèmes informatiques. Organisées autour de trois pôles de compétences - Études, Expertise et Production - les DSI sont soutenues par des fonctions administratives et pilotées par un comité directeur. Ces trois pôles comprennent plusieurs fonctions clés :

- Le pilotage de la DSI : Il vise à aligner les systèmes d'information sur les exigences de la direction générale et à déterminer les orientations stratégiques de la DSI.

- L'assistance utilisateurs : Cette fonction assure le support quotidien aux utilisateurs en lien avec les systèmes d'information.

- Les fonctions transverses : Elles garantissent le bon déroulement de la gestion du SI, notamment en pilotant les projets et en définissant les normes et méthodes à appliquer.

La gestion des risques est une composante intégrante de la vie des entreprises. Elle se prévoit en amont et implique souvent le département informatique. La DSI joue un rôle crucial dans cette gestion en assurant plusieurs missions :

- Préparer en amont et anticiper la gestion des risques.

- Assurer la continuité d'activité et veiller à la mise en conformité de l'entreprise.

- Participer à l'élaboration du plan de continuité d'activité en intégrant toutes les parties prenantes de l'entreprise.

- Collaborer avec les gestionnaires de risques pour détecter, évaluer et analyser les risques et leurs impacts.

La DSI est également essentielle dans la gestion de la sécurité de l'information, notamment face aux risques technologiques qui sont devenus des risques opérationnels. Elle peut s'appuyer sur son expertise et ses compétences pour automatiser certains processus liés à la gestion des risques, tels que la cartographie des risques ou la détection de fraudes.

En conclusion, la DSI est un acteur clé dans la gestion des risques et la continuité d'activité à l'ère numérique. Son rôle est indispensable pour garantir le bon fonctionnement des systèmes d'information et assurer la sécurité des données, tout en contribuant à la performance globale de l'entreprise.

Conclusion du premier chapitre

La gestion des risques liés aux technologies de l'information et aux systèmes d'information est cruciale pour toute entreprise. Elle implique l'identification, l'évaluation et la gestion des risques opérationnels associés à ces domaines. En optimisant les ressources consacrées à la sécurité, elle permet de contrôler les conséquences négatives des risques et

de transformer ces derniers en opportunités profitables pour l'entreprise. Les managers doivent être impliqués dans ce processus afin de comprendre les coûts associés aux risques et de mettre en place des mesures de protection appropriées. Une gestion proactive des risques permet aux organisations de mieux assumer leur responsabilité et de rester conscientes des défis posés par les technologies de l'information.

CHAPITRE II

Enterprise Risk Management et la fonction d'audit

CHAPITRE II : Enterprise Risk Management et la fonction d’audit

Le Enterprise Risk Management (ERM), selon l'IIA, est un processus structuré et continu appliqué à l'ensemble de l'organisation pour identifier, évaluer et répondre aux risques, ainsi qu'aux opportunités, affectant la réalisation des objectifs. Il est crucial pour toutes les entreprises car il permet de déterminer le niveau d'incertitude et de risque acceptable.

Parmi les référentiels normatifs relatifs à la gestion des risques, la norme ISO 31000 « Risk Management » est mise en avant dans cette section en raison de son processus complet et détaillé applicable à tous types d'entreprises.

Ensuite, nous abordons le contrôle interne, un ensemble de processus visant à garantir un degré raisonnable de confiance dans la réalisation des objectifs, et sa relation avec le processus ERM dans le dispositif de gouvernance et de gestion des risques.

Nous clarifions également le rôle et les missions des auditeurs internes dans la gestion des risques, en mettant en évidence les responsabilités spécifiques du management des risques qui ne doivent pas être assumées par les auditeurs internes selon les normes de l'IIA.

Enfin, nous examinons l'implication correcte des auditeurs internes dans l'ERM et son évaluation, soulignant comment cela peut aider l'organisation à améliorer ce processus et à optimiser sa performance globale.

SECTION 1 : LE PROCESSUS DE MANAGEMENT DES RISQUES « ERM » SELON L'ISO 31000

Intégré dans le cadre de la restructuration continue et de la gestion continue, le processus de gestion des risques d'entreprise (ERM) est une composante essentielle de l'ensemble du dispositif de gestion des risques. Les entreprises l'adaptent et le mettent en place pour répondre aux divers risques auxquels elles sont confrontées.

1. Le concept ERM :

Face aux risques émergents, l'entreprise déploie un processus complet de gestion des risques, impliquant une application systématique de politiques, de procédures et de pratiques dans les domaines de la communication, de la consultation, de l'établissement du contexte, de l'appréciation, du traitement, du suivi, de la revue, de l'enregistrement et du compte rendu des risques (ISO 31000, 2018). Ce processus de gestion des risques constitue une méthodologie clairement définie pour identifier les risques et les opportunités présents, comprendre leur impact potentiel sur un projet ou une organisation, et élaborer des réponses adaptées. L'ERM représente l'approche principale pour gérer et optimiser les risques, permettant à une organisation de déterminer le niveau d'incertitude et de risque acceptable.

Pour que le processus de gestion des risques soit efficacement mis en place, il est essentiel de bénéficier du soutien et de l'engagement de la direction générale, de prendre en considération la valeur ajoutée que ce processus apporte à l'organisation, de coopérer avec les managers fonctionnels et opérationnels, de disposer d'informations fiables, et de faire preuve d'objectivité dans l'identification et l'évaluation des risques. En outre, il est impératif, dans un premier temps, de définir clairement les objectifs afin que la gestion des risques puisse identifier les événements potentiels susceptibles d'affecter leur réalisation. Cette fixation des objectifs est également essentielle pour garantir une mise en place efficace d'un processus visant à les atteindre (CORDEL, 2013).

1.1. Objectifs et avantages :

Les objectifs du processus de gestion des risques sont variés. Ils incluent principalement l'amélioration de la rentabilité et de la productivité, la maîtrise des coûts et des délais, ainsi que l'assurance de la qualité des produits. Cela se réalise par une analyse et une gestion

Complète des risques, ainsi que par la proposition et la coordination de plans d'action. Ce processus est clairement un outil décisionnel essentiel pour les dirigeants d'entreprise.

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

- Identifier et hiérarchiser rapidement les risques auxquels l'organisation est confrontée.
- Recenser de manière exhaustive les risques majeurs pouvant affecter l'organisation, en les décrivant précisément en fonction de leur impact et de leur probabilité d'occurrence grâce à l'élaboration d'une cartographie des risques.
- Déterminer un niveau de risque acceptable pour l'organisation, établissant ainsi une limite ou un seuil au-delà duquel la sécurité de l'organisation serait compromise.
- Définir et mettre en œuvre des mesures d'atténuation et de maîtrise des risques, en tenant compte des seuils jugés acceptables.
- Assurer un suivi permanent des activités afin de réévaluer périodiquement les risques et l'efficacité des contrôles, et garantir une cohérence globale de la méthode de gestion des risques d'une activité à l'autre.
- Informer périodiquement le conseil et la direction générale des résultats du processus de management des risques.
- Maintenir un niveau de qualité des rapports internes et externes.
- Alimenter le plan d'audit interne.
- Améliorer le système de communication entre toutes les parties concernées en élaborant un dispositif commun sur la politique de risque adoptée par l'organisation.

En général, le processus de management des risques offre l'avantage de promouvoir ou de renforcer une culture du risque au sein de l'entreprise et de partager les meilleures pratiques en fournissant des outils et des méthodes aux managers pour les aider à identifier, évaluer et traiter les risques.

1.2.Limite :

D'après DUMORA (2017), le dispositif de management des risques doit être exhaustif pour englober tous les risques auxquels l'entreprise est exposée. Il doit être cohérent afin d'harmoniser la stratégie de risque des actionnaires et des managers avec les décisions opérationnelles prises par l'ensemble des collaborateurs. De plus, ce dispositif doit être homogène pour éviter une protection excessive face à un risque au détriment d'un autre, et intégré à l'activité opérationnelle de l'entreprise pour être accessible à tous les collaborateurs. Enfin, il doit être clair et compréhensible, se présentant comme un système d'information et des procédures de décision faciles à assimiler pour tous les acteurs.

Cependant, malgré son importance, le processus de management des risques comporte des limites, selon CORDEL (2013) :

- La difficulté à concilier les objectifs de l'entreprise avec ceux des individus chargés de les mettre en œuvre.
- Les contradictions entre les objectifs stratégiques, opérationnels ou de conformité.
- La présence d'objectifs parfois irréalistes par rapport aux ressources disponibles.
- Des lacunes dans la communication des objectifs.
- L'autosuffisance des objectifs sans possibilité de mesurer leur réalisation.
- Des limitations dans la cartographie des risques, notamment la compression des intervalles et l'hypothèse d'intervalles réguliers, ainsi que l'interdépendance supposée des risques.

1.3. Outils :

D'après CORDEL (2013), une variété d'outils de gestion des risques existe, chacun étant adapté à la diversité des projets. Voici quelques-uns :

- ✓ **Les contrôles :**

Le dispositif de contrôle interne des risques couvre toutes les filières de risque et s'appuie sur trois niveaux : les contrôles intégrés dans les opérations, la validation des contrôles de premier niveau (contrôle permanent), et les contrôles indépendants effectués dans le cadre de missions d'audit périodiques (contrôles ponctuels).

- ✓ **Les stress tests :**

Ces tests évaluent la résilience de l'entreprise face à diverses situations telles que les crises internes, économiques, politiques, naturelles ou technologiques. Ils permettent de mesurer l'impact de ces situations sur les risques de marché, de souscription, de crédit et opérationnels.

- ✓ **Le reporting** :

Chaque entreprise doit répondre à des exigences de reporting spécifiques dans chaque territoire où elle opère. Le reporting permet de rendre compte périodiquement des performances et aide à la prise de décisions. Des nouveaux outils de reporting comme ceux proposés par Solvabilité II deviennent également cruciaux pour le pilotage interne de l'entreprise.

- ✓ **Les transferts de risque :**

Ces techniques visent à gérer les risques et la solvabilité au-delà des stratégies de développement. Par exemple, une entreprise peut utiliser des traités de réassurance élargis pour réduire son exposition aux risques dans certains marchés.

D'autres outils sont également disponibles pour améliorer la gestion des risques, tels que les techniques d'animation de groupe, les méthodes d'analyse décisionnelle comme le « Reference Class Forecasting », les matrices de risques, les formulaires et registres, ainsi que la formation continue.

2. Les acteurs de l'ERM :

La coordination des activités et des actions des acteurs impliqués dans le processus de management des risques est cruciale en raison de leur nombre (IFACI, 2003). Voici les principaux acteurs :

- ✓ **Le conseil :**

Il surveille l'efficacité du processus et s'assure qu'il est régulièrement évalué.

- ✓ **La direction générale :**

Responsable de la conception, de la mise en œuvre et du suivi du processus au sein de l'entreprise.

- ✓ **Les comités spécialisés du conseil :**

Tels que le comité d'audit et le comité des risques, ils examinent les risques significatifs et dirigent la prévention et la maîtrise des risques.

- ✓ **Les auditeurs internes :**

Ils évaluent et contribuent à l'amélioration du processus de gestion des risques.

- ✓ **Le Risk manager :**

Chargé de communiquer le processus aux opérationnels et d'aider à définir la stratégie de gestion des risques.

- ✓ **La direction opérationnelle et fonctionnelle :**

  Responsable du traitement des risques dans leur domaine et de la détermination du niveau de risque acceptable.

- ✓ **Le contrôleur de gestion :**

  Contribue au déploiement de la cartographie des risques et au suivi des actions préventives.

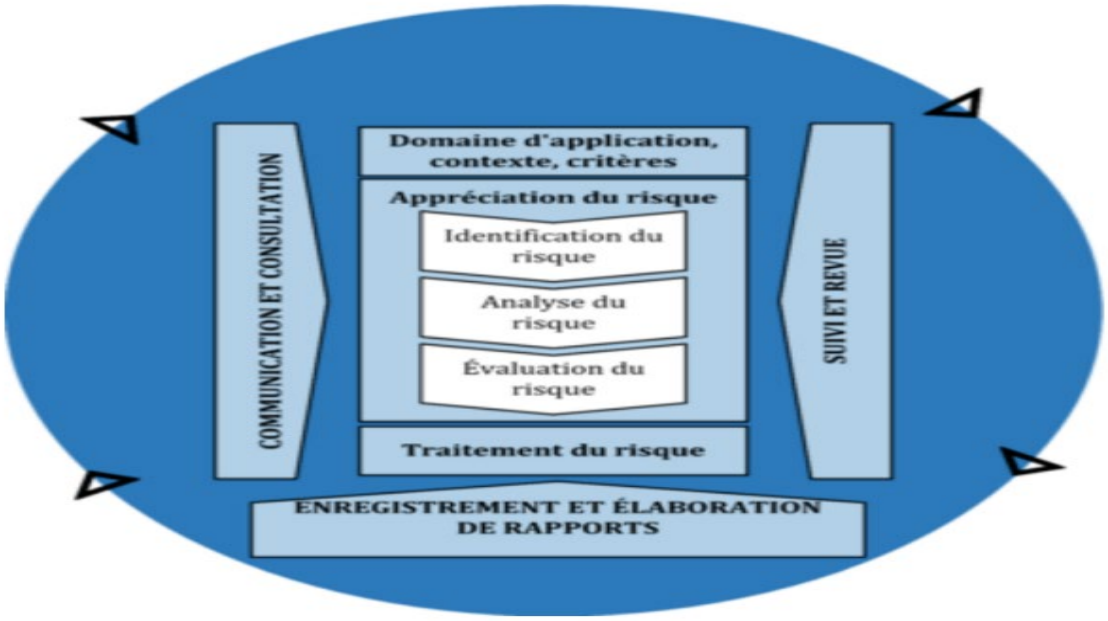
- ✓ **Les commissaires aux comptes ou les auditeurs externes :**

  Ils fournissent des modèles et des outils d'analyse des risques dans le cadre de leur mission de certification des comptes.

3. **Phases du processus de management du risque :**

   L'ISO 31000, édition 2018, offre une approche générale et globale du management des risques pour les organismes, indépendamment de leur type ou de leur contexte spécifique. Cette norme peut être appliquée à toutes les activités et à toutes les décisions prises à différents niveaux au sein de l'organisation. Elle propose un processus en cinq étapes ou activités clés, tel qu'illustré dans la figure ci-dessous.

Figure 7 : Le processus de management des risques selon la norme ISO 31000, tirée de "ISO 31000:2018 (Fr) Management du risque — Lignes directrices".



Source : https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:f

3.1.Communication et consultation :

La première phase du processus de gestion des risques implique une coordination entre la communication et la consultation pour sensibiliser et guider les parties prenantes dans la compréhension des risques et des principes de prise de décision. Cela nécessite des échanges d'informations clairs et pertinents, ainsi que l'établissement d'hypothèses de travail communes avec les parties concernées, internes et externes, pour assurer une vision partagée du dispositif de gestion des risques. La communication et la consultation rassemblent diverses expertises et perspectives lors de l'évaluation des risques, tout en fournissant les informations nécessaires à la surveillance des risques et à la prise de décision.

3.2. Etablissement du contexte :

cette phase du processus de gestion des risques vise à comprendre l'environnement dans lequel l'organisation évolue, en tenant compte des contraintes et des opportunités externes (sociales, culturelles, réglementaires, politiques et économiques) ainsi que des facteurs internes tels que la stratégie, les objectifs, les ressources et les outils techniques. L'objectif est

d'adapter le processus de gestion des risques pour permettre une évaluation et un traitement efficaces en définissant clairement le contexte organisationnel.

elle inclut la définition des critères de risque pour reconnaître et évaluer l'importance des risques, en tenant compte des perceptions des parties prenantes et des exigences légales ou réglementaires.

Pour établir ces critères, plusieurs éléments doivent être pris en compte :

- La nature et le type d'incertitudes susceptibles d'affecter les résultats et les objectifs ;
- La manière dont les conséquences et les probabilités de ces risques sont définies et mesurées ;
- Les facteurs temporels ;
- La cohérence dans l'utilisation des mesures ;
- La méthode de détermination du niveau de risque ;
- La prise en compte des combinaisons et des séquences de plusieurs risques ;
- La capacité de l'entreprise à gérer les risques.

La définition du périmètre d'application, du contexte et des critères permet d'adapter le processus de gestion des risques pour une évaluation efficace et un traitement approprié. Cela implique de définir clairement le champ d'application du processus et de comprendre à la fois le contexte interne et externe.

3.3.Appréciation du risque :

L'appréciation des risques est un processus global impliquant l'identification, l'analyse et l'évaluation des risques. Elle doit être menée de manière systématique, collaborative et itérative, en utilisant les connaissances et les opinions des parties prenantes, ainsi que les meilleures informations disponibles, avec la possibilité d'approfondir par une enquête si nécessaire.

3.3.1. Identification du risque :

L'élaboration d'une cartographie des risques vise à identifier les obstacles potentiels ou les opportunités qui pourraient empêcher une entreprise d'atteindre ses objectifs. La norme ISO 31000 se concentre sur les risques liés à la non-saisie d'une opportunité, couvrant les dimensions du Corporate et du business Risk management. Pour cela, il faut prendre en

compte de nombreux facteurs tels que les sources de risque, les causes et événements, les menaces et opportunités, les vulnérabilités et capacités, les indicateurs de risque émergents, les conséquences et leurs impacts sur les objectifs, ainsi que les facteurs temporels. L'identification des risques, qu'ils soient sous contrôle ou non, est essentielle, car ils peuvent entraîner diverses conséquences tangibles ou intangibles.

3.3.2. Analyse du risque :

L'analyse des risques vise à comprendre pleinement la nature du risque en considérant son origine, la probabilité des événements, la nature et l'ampleur de leurs conséquences, ainsi que l'efficacité des moyens de maîtrise. Elle permet de prendre des décisions éclairées quant au traitement du risque en élaborant des stratégies appropriées. Cette phase peut être simple ou complexe en fonction de la disponibilité des informations, des divergences d'opinions sur le risque et des jugements à intégrer. Les techniques d'analyse peuvent être qualitatives, quantitatives ou une combinaison des deux, en fonction de la gravité des conséquences des événements incertains. Pour être efficace, il est crucial de considérer divers facteurs tels que la probabilité et les conséquences des événements, la complexité des facteurs impliqués, les considérations temporelles, l'efficacité des mesures de maîtrise existantes, ainsi que les niveaux de sensibilité et de confiance dans les données disponibles.

3.3.3. Évaluation du risque :

L'évaluation des risques consiste à comparer les résultats de l'analyse des risques avec des critères préétablis, afin de prendre des décisions sur les actions à entreprendre concernant le risque. Elle tient compte du contexte et des conséquences perçues par les parties prenantes internes et externes. Les décisions peuvent aller de ne rien faire à maintenir les mesures existantes, en passant par l'examen des options de traitement et la réalisation d'une analyse plus poussée pour mieux comprendre le risque et réévaluer les objectifs. Les résultats de cette évaluation doivent être enregistrés, communiqués et validés aux niveaux appropriés de l'organisation.

3.4. Traitement du risque :

L'objectif de cette étape est de sélectionner les options et les actions pour éliminer ou réduire le risque à un niveau acceptable. On évalue également l'efficacité des actions déjà entreprises pour traiter le risque et on considère un traitement complémentaire si le risque résiduel est

inacceptable. Plusieurs options sont envisageables, comme l'arrêt ou le démarrage d'une activité à risque, la suppression de la source du risque, le partage ou le transfert du risque via des contrats d'assurance, ou la modification de la vraisemblance et des conséquences du risque. Le choix de l'action à entreprendre doit tenir compte des obligations de l'organisme, des avantages par rapport aux coûts, des valeurs des parties prenantes et des risques secondaires potentiels. Un plan intégré au processus de management est établi pour détailler la manière et l'ordre dans lesquels les actions seront appliquées, avec justification, délais, responsables, ressources nécessaires, mesures de performance et suivis requis.

3.5.Surveillance et revue :

La phase de suivi et de revue vise à garantir l'efficacité du processus de gestion des risques. Elle implique la mise en place d'un système d'information pour suivre périodiquement les risques et définir les responsabilités. La surveillance est effectuée à toutes les étapes pour s'assurer de l'efficacité des contrôles et détecter les risques émergents ou les changements de contexte. Cette phase se composent de cinq étapes similaires à celles de l'Analyse de Risques Majeurs (ARM) :

- Identification et analyse des risques
- Étude des outils de contrôle des risques
- Choix optimal des outils en fonction des critères de minimisation des impacts
- Mise en œuvre des décisions, y compris la budgétisation
- Reporting et monitoring

Les résultats du processus de gestion des risques sont documentés et rapportés pour informer les décisions, améliorer la gestion des risques et faciliter la communication avec les parties prenantes. Cette phase inclut la rédaction de rapports, en tenant compte des coûts, des besoins des parties prenantes et de la pertinence des informations. Les résultats peuvent conduire à différentes stratégies : accepter les risques, les éviter, les atténuer ou les transférer à d'autres parties.

SECTION 2 : LA GESTION DES RISQUES ET LR CONTROLE INTERNE

Chaque entreprise s'efforce de mettre en place des systèmes de gestion des risques et de contrôle interne adaptés à ses propres caractéristiques, agissant de manière complémentaire pour assurer la maîtrise de ses activités. Le dispositif de gestion des risques a pour objectif

d'identifier et d'analyser les principaux risques auxquels l'entreprise est confrontée, en utilisant des mécanismes de contrôle relevant du système de contrôle interne. Cette section examinera le contrôle interne et sa relation avec la gestion des risques d'entreprise (ERM).

1. Principes généraux du CI :

Le contrôle interne, selon l'AMF (2010), est un dispositif mis en place par une organisation pour maîtriser ses activités, rendre ses opérations efficaces et optimiser l'utilisation de ses ressources. Il vise à prendre en compte les risques significatifs, assurer la conformité aux lois et règlements, et garantir le bon fonctionnement des processus internes, y compris la protection des actifs et la fiabilité des informations financières. Il englobe toutes les initiatives de la direction, telles que la définition de la stratégie, la gestion des risques et le suivi des performances.

1.1. Composantes :

Le cadre de référence de l'AMF (2010) propose cinq composantes pour le dispositif de contrôle interne :

- **Organisation :** Cela implique une définition claire des responsabilités, des ressources adéquates et des compétences nécessaires. Il s'appuie sur des systèmes d'information, des procédures et des pratiques appropriées. Les responsabilités doivent être clairement définies et communiquées, conformément au principe de la séparation des tâches. Une politique de gestion des ressources humaines est essentielle pour garantir que l'entreprise dispose du personnel compétent et formé.
- **Diffusion interne d'informations :** Les informations diffusées doivent être pertinentes et fiables, permettant à chacun d'exercer ses responsabilités. La société doit disposer de processus de communication efficaces pour diffuser ces informations de manière opportune aux acteurs concernés.
- **Gestion des risques** : Cette composante vise à recenser, analyser et traiter les principaux risques identifiés par rapport aux objectifs de l'entreprise.
- **Activités de contrôle :** Ces activités doivent être adaptées aux enjeux propres à chaque processus et conçues pour s'assurer que les mesures nécessaires sont prises pour maîtriser les risques. Elles peuvent être préventives ou de détection, manuelles ou informatiques, et s'appliquent à tous les niveaux de l'organisation.

- **Surveillance permanente :** Le dispositif de contrôle interne doit faire l'objet d'une surveillance continue et d'un examen régulier pour vérifier sa pertinence et son adéquation aux objectifs de l'entreprise.

1.2. Objectifs :

D'après les directives de l'AMF (2010), le dispositif de contrôle interne vise principalement à :

- **Assurer le respect des lois et réglementations :** Il est primordial que l'entreprise dispose d'une organisation permettant de comprendre et de suivre les règles imposées par les lois et règlements, ainsi que de les intégrer dans ses procédures internes, et de former ses collaborateurs à leur respect.
- **Mettre en œuvre les directives et orientations de la direction générale :** Cela implique de communiquer aux collaborateurs les attentes et les libertés d'action qui leur sont accordées, en tenant compte des objectifs de la société et des risques encourus.
- **Garantir le bon fonctionnement des processus internes :** Ceci inclut notamment les processus visant à protéger les actifs de l'entreprise, tels que les processus opérationnels, industriels, commerciaux et financiers, en établissant des normes de fonctionnement et en mettant en place des indicateurs de suivi.
- **Assurer la fiabilité des informations financières :** Cela nécessite la mise en place de procédures de contrôle interne pour garantir l'exactitude des opérations enregistrées, avec notamment une séparation des tâches, une description des fonctions pour identifier les sources des informations, et un système comptable interne conforme aux principes comptables généralement admis.

2. Articulation entre CI et ERM :

Selon l'Autorité des Marchés Financiers (AMF, 2010), le contrôle interne et le processus de gestion des risques sont interdépendants. Le processus de gestion des risques repose sur le contrôle interne pour mettre en place des mesures garantissant le bon fonctionnement de l'entreprise et pour identifier et évaluer les principaux risques auxquels elle est exposée. De son côté, le contrôle interne s'appuie sur le processus de gestion des risques pour repérer et maîtriser ces risques.

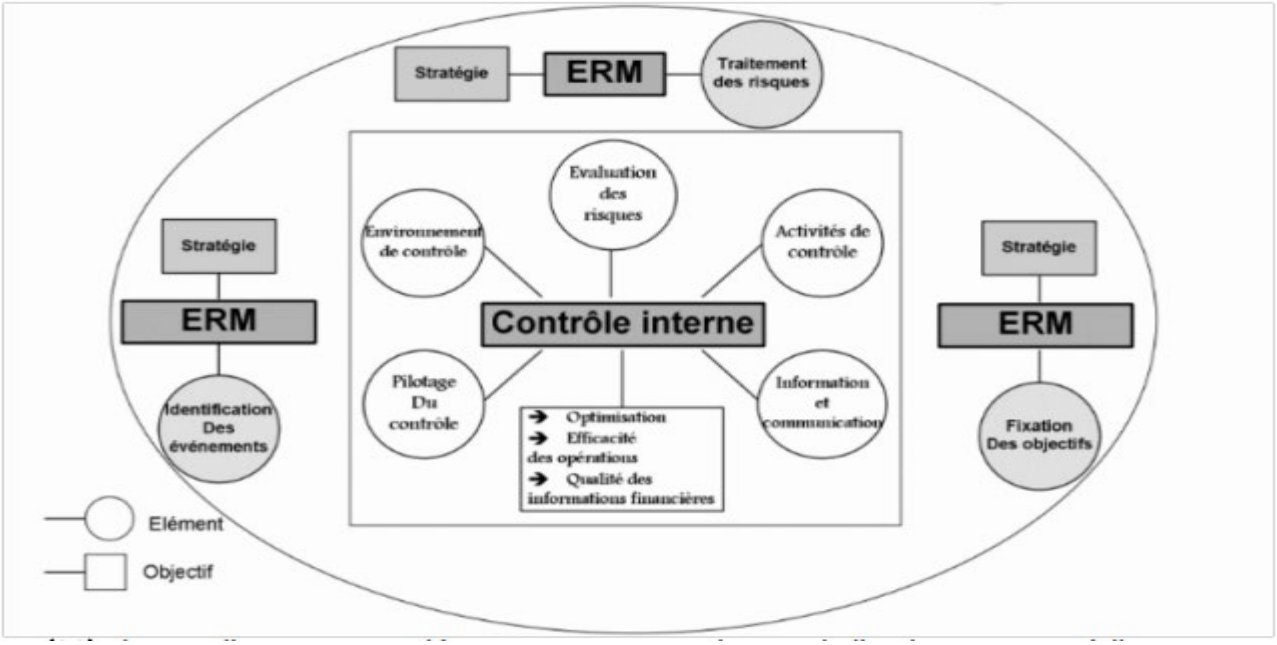
La relation entre ces deux dispositifs est influencée par la culture de gestion des risques et de contrôle propre à chaque entreprise, par le style de management adopté et par les valeurs éthiques de l'organisation.

Dans son analyse, Sourour (2018) a examiné la relation entre le contrôle interne et le processus de gestion des risques en mettant en avant deux concepts : la complémentarité et la substitution.

2.1. La complémentarité entre CI et ERM :

L'Enterprise Risk Management (ERM) est une évolution du contrôle interne, conçue comme un dispositif de gouvernance d'entreprise visant à atténuer les risques auxquels elle est confrontée. Selon les schémas présentés, l'ERM enrichit les composantes du contrôle interne en incluant trois nouveaux paramètres, notamment le traitement des risques, en plus d'un quatrième objectif qui est la stratégie.

Figure 08 : Le contrôle interne et l'ERM se complètent, extrait de "La contribution de



l'auditeur interne à l'Enterprise Risk Management : résultats d'une étude exploratoire

Source : Sourour, 2018, p. 05.

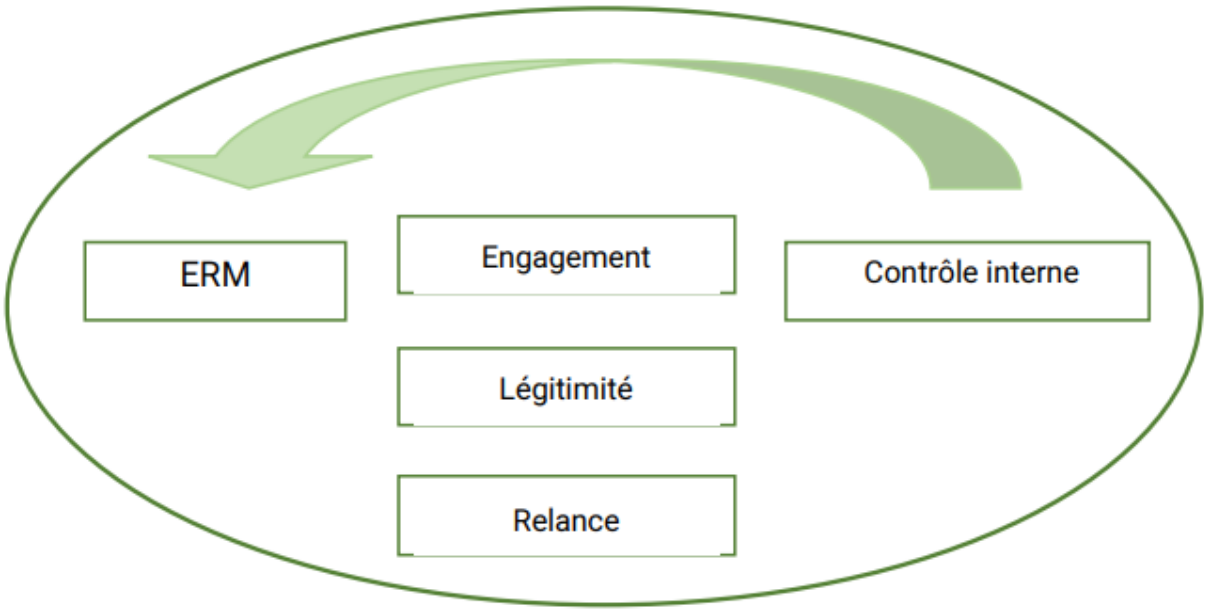
https://www.researchgate.net/publication/33125105

Après avoir développé le cadre de l'ERM, le COSO a clairement indiqué que la fonction d'audit interne devrait assister la direction dans l'évaluation de l'efficacité des risques d'entreprise grâce au contrôle interne.

2.2. La substitution entre ERM et CI :

À la conclusion de son étude, Sourour (2018) a rejeté l'idée que l'ERM est simplement une extension du contrôle interne en ce qui concerne sa contribution à la fonction d'audit interne. Il a plutôt adopté l'hypothèse de la substitution. Bien que le contrôle interne soit crucial pour la fiabilité des informations, il présente plusieurs lacunes. Une entreprise sans fonction d'audit interne aura du mal à produire un reporting efficace sur le CI. Une étude sur l'efficacité du contrôle interne réalisée par l'AI a révélé des lacunes dans le contenu informationnel des rapports, remettant en question son amélioration potentielle de la fiabilité des informations. Ainsi, l'accent mis sur la gestion des risques a conduit à substituer le contrôle interne par l'ERM. L'engagement de la direction envers l'AI, la légitimité de sa contribution à l'ERM, et le renouveau du contrôle interne expliquent ce passage de la substitution du CI vers l'ERM.

Figure(09) : Le remplacement du contrôle interne par l'ERM selon "La contribution de



l'auditeur interne à l'entreprise Risk Management : résultats d'une étude exploratoire"

Source : Sourour.2018, p05

https://www.researchgate.net/publication/331251058

la DG doit garantir la coordination entre le CI et l'ERM pour mener à bien les activités suivantes : cartographie et évaluation des risques, définition et évaluation des activités de contrôle, plans de remédiation, pilotage et diffusion de l'information, et supervision continue. Le modèle des "trois lignes de défense" propose des recommandations précieuses sur la répartition des responsabilités en matière de gestion des risques et de contrôle interne.

3. Les trois lignes de défense «3 LoD» :

Le modèle des 3LoD est utilisé pour évaluer l'efficacité de la gestion des risques, car il offre une méthode simple et efficace pour s'assurer que l'ERM et le contrôle interne sont coordonnés et complémentaires au sein d'une organisation.

3.1. La première ligne de défense :

La première ligne de défense, composée de la direction opérationnelle de l'organisation, a pour mission essentielle d'identifier, d'évaluer, de contrôler et de réduire les risques en mettant en place un dispositif de contrôle adapté aux processus sous sa responsabilité. Cette fonction gère le risque tout en garantissant la maîtrise des activités quotidiennes grâce à des pratiques efficaces de gestion des risques et en communiquant les informations pertinentes à la deuxième ligne de maîtrise. Selon le modèle des trois lignes de défense de l'IIA, ses responsabilités incluent :

- Orienter et diriger les actions, notamment en matière de gestion des risques, et optimiser l'utilisation des ressources disponibles pour atteindre les objectifs de l'organisation.
- Maintenir un dialogue continu avec l'organe de gouvernance et lui fournir des rapports sur les résultats prévus et réalisés par rapport aux objectifs de l'organisation, ainsi que sur les risques.
- Établir et maintenir les structures et les processus appropriés pour la gestion des opérations et des risques, y compris le contrôle interne.
- Assurer le respect des exigences légales, réglementaires et éthiques.

3.2. La deuxième ligne de défense :

En plus des services fonctionnels responsables de domaines d'expertise, la deuxième ligne intègre les fonctions de gestion des risques, de contrôle interne, d'assurance et de conformité,

contribuant ainsi à dynamiser le dispositif global de maîtrise des risques. Leur mission englobe :

- Soutenir les opérationnels dans l'identification et l'évaluation des principaux risques de leur domaine d'expertise, ainsi que dans la conception de contrôles adaptés.
- Élaborer des politiques et des procédures spécifiques à chaque domaine d'activité.
- Promouvoir les meilleures pratiques et favoriser les échanges, tout en assurant une surveillance et un suivi efficaces des processus en place.

Ces services détiennent une expertise unique dans l'analyse organisationnelle et les compétences clés en matière de contrôle, ce qui facilite la communication d'informations pertinentes sur les risques à l'ensemble de l'organisation.

Le modèle des trois lignes de défense de l'IIA 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, y compris le contrôle interne, afin de favoriser le développement, la mise en œuvre et l'amélioration continue des pratiques de gestion des risques.
- Produire des analyses et des rapports sur l'efficacité de la gestion des risques, incluant le contrôle interne.

La distinction entre les premières et deuxièmes lignes dans le modèle des trois lignes de défense de l'IIA est cruciale pour l'organisation. La première ligne assure les fonctions de support et fournit les produits et services aux clients, tandis que la deuxième se concentre sur les activités de soutien à la gestion des risques. Certains rôles de la deuxième ligne peuvent être confiés à des spécialistes pour apporter une expertise complémentaire et des critiques constructives, tandis que d'autres sont axés sur des objectifs précis en matière de gestion des risques.

3.3. La troisième ligne de défense :

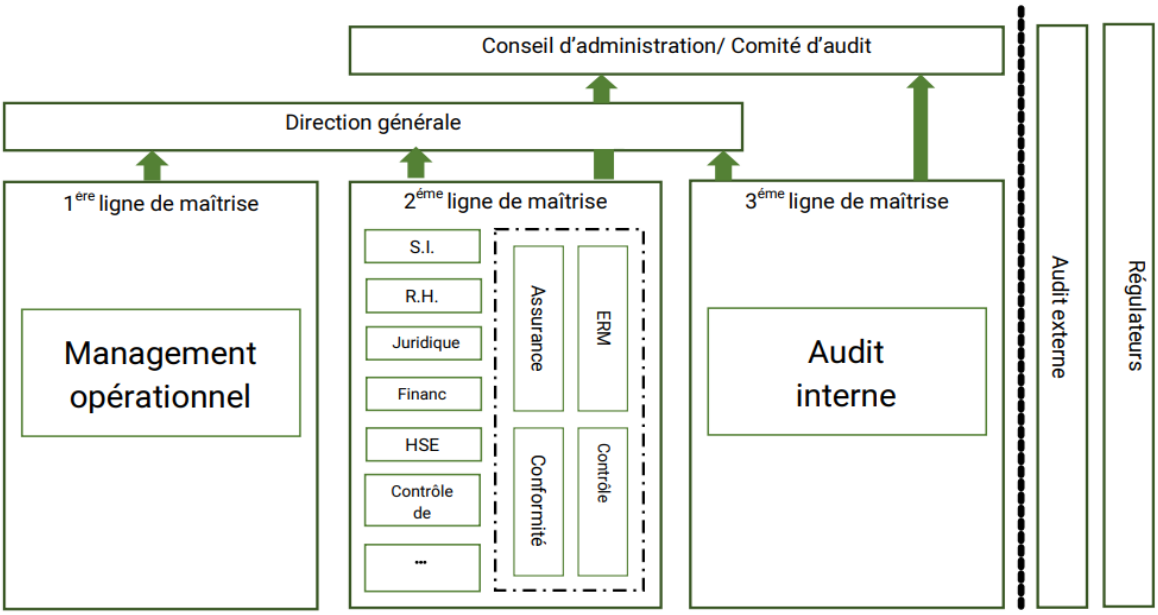
Dans une approche axée sur le risque, la troisième ligne de défense, équivalente à l'audit

interne, fournit une assurance indépendante sur l'efficacité des deux premières lignes de maîtrise et de la gouvernance de la gestion des risques. Elle assure une assurance globale, objective et indépendante aux organes de surveillance et à la direction générale de l'organisation. La fonction de la troisième ligne doit être directement rattachée au plus haut niveau de l'organe de gouvernance, avec un accès total aux ressources nécessaires pour exercer ses fonctions en toute indépendance et objectivité.Le rôle de l'audit interne, tel que défini par l'IIA, implique plusieurs points clés :

- Rendre compte en premier lieu à l'organe de gouvernance et préserver son indépendance vis-à-vis du management.
- Fournir une assurance et des conseils indépendants et objectifs au management et à l'organe de gouvernance sur l'efficacité de la gouvernance et de la gestion des risques, y compris le contrôle interne, afin de contribuer à la réalisation des objectifs de l'organisation et de promouvoir l'amélioration continue.
- Alerter l'organe de gouvernance en cas d'atteinte à son indépendance et à son objectivité, et prendre les mesures de protection nécessaires.

Le schéma suivant illustre ces trois lignes de défense et leur relation avec la direction générale et le conseil d'administration.

Figure (10) : Les trois lignes de défense d'après "Trois lignes de Maîtrise pour une meilleure



performance", IFA, 2013, AMRAE–IFAC,

Source : 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. 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 ;
- La pertinence et l'adéquation des modalités de traitement des risques avec l'appétence de l'organisation pour le risque ;
- La communication opportune des informations relatives aux risques au sein de l'organisation, pour permettre aux collaborateurs, à leur hiérarchie et au conseil d'exercer leurs responsabilités.

Pour étayer cette évaluation, l'audit interne peut se baser sur les informations collectées lors de différentes missions. Une synthèse des résultats de ces missions permet de mieux comprendre le processus de gestion des risques de l'organisation et son efficacité. La surveillance de ce processus peut être assurée par le biais d'activités de gestion courantes, d'évaluations distinctes ou par une combinaison des deux méthodes.

La série de normes IIA 2120 se compose de cinq points :

- 2120.A1 : L'audit interne doit évaluer les risques associés à la gouvernance, aux opérations et aux systèmes d'information de l'organisation par rapport aux objectifs stratégiques, à la fiabilité des informations financières et opérationnelles, à l'efficacité des opérations et programmes, à la protection des actifs, et au 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 : Dans le cadre des missions de conseil, les auditeurs internes doivent couvrir les risques associés aux objectifs de la mission et rester vigilants quant à l'existence d'autres risques potentiellement significatifs.
- 2120. C2 : Les auditeurs internes doivent utiliser leurs connaissances des risques acquises lors des missions de conseil pour évaluer les processus de gestion des risques de l'organisation.
- 2120. C3 : Lorsqu'ils aident la direction à concevoir et à améliorer les processus de gestion des risques, les auditeurs internes doivent s'abstenir d'assumer une responsabilité opérationnelle dans ce domaine.

1.2.Concepts de base :

Selon l'IFACI (2002), l'audit interne est une activité indépendante et objective qui fournit à une organisation une assurance sur le degré de maîtrise de ses opérations, tout en offrant des conseils pour les améliorer, et en contribuant à la création de valeur ajoutée.

Il contribue à la réalisation des objectifs d'une entreprise en évaluant de manière systématique et méthodique ses processus de gestion des risques, de contrôle et de gouvernance d'entreprise, et en proposant des recommandations pour renforcer leur efficacité.

1.2.1. Principes de l'audit interne :

En 2012, l'IFACI a élaboré un référentiel professionnel présentant les exigences auxquelles la direction de l'audit interne doit se conformer. Ce référentiel se décline en trois formes distinctes :

Exigences de moyens :

- Assurer l'indépendance du service d'audit interne.
- Établir une charte définissant clairement les missions et responsabilités.
- Respecter le code de déontologie et travailler avec objectivité.
- Avoir des compétences adéquates et les mettre en œuvre diligemment.
- Garantir des ressources adéquates et les utiliser efficacement.
- Acquérir et maintenir les compétences nécessaires.
- Établir des règles et procédures encadrant l'activité d'audit interne.

Exigences de prestation :

- Évaluer la gouvernance et les processus de gestion des risques et de contrôle interne.
- Établir un plan d'audit basé sur les risques.
- Communiquer le plan et les besoins aux parties concernées.
- Déterminer les ressources nécessaires pour chaque mission.
- Informer le management sur le déroulement de la mission.
- Élaborer un plan de mission et un programme de travail.
- Identifier, analyser et documenter les informations pertinentes.
- Communiquer les résultats de la mission de manière appropriée.
- Mettre en place un suivi des actions correctives.

- Coordonner les activités avec les prestataires internes et externes.
- Rendre compte périodiquement des résultats aux parties concernées.

Exigences de pilotage :

- Piloter le service d'audit interne pour apporter de la valeur ajoutée.
- Superviser les missions d'audit interne de manière appropriée.
- Mettre en place un programme d'assurance qualité pour contrôler l'efficacité de l'audit interne.
- Indiquer si une mission n'a pas été menée conformément aux normes.

1.2.2. Normes d'audit interne :

Les normes d'audit interne, élaborées par l'IIA (Institute of Internal Auditors), sont présentées par l'IFACI (2012) de manière détaillée et commentée, et se composent de trois catégories : les normes de qualification, de fonctionnement et de mise en œuvre.

Objectifs des normes :

- Définir les principes fondamentaux à suivre dans la pratique de l'audit interne.
- Fournir un cadre de référence pour diverses activités d'audit interne visant à apporter une valeur ajoutée.
- Établir des critères pour évaluer le fonctionnement de l'audit interne.
- Favoriser l'amélioration des processus organisationnels et des opérations.

Normes de qualification : énoncent les critères que doivent respecter les organisations et les professionnels impliqués dans l'audit interne :

- La norme 1000 « Mission, pouvoirs et responsabilités » exige que la mission, les pouvoirs et les responsabilités de l'audit interne soient clairement définis dans une charte, approuvés par le conseil.
- La norme 1100 « Indépendance et objectivité » stipule que l'audit interne doit être indépendant et que les auditeurs doivent agir avec objectivité.

- La norme 1200 « Compétence et conscience professionnelle » impose que les missions soient exécutées avec compétence et professionnalisme.

- La norme 1300 « Programme d'assurance et d'amélioration qualité » requiert que le responsable de l'audit interne élabore et mette à jour un programme d'assurance qualité couvrant tous les aspects de l'audit interne. Ce programme vise à garantir un contrôle continu de l'efficacité de l'audit interne et à promouvoir son amélioration, tout en assurant sa conformité aux normes et au code de déontologie.

Les normes de fonctionnement : décrivent les activités de l'audit interne et fixent des critères de qualité pour évaluer les services fournis :

- Norme 2000 « Gestion de l'audit interne » : Le responsable de l'audit interne doit diriger cette fonction pour qu'elle apporte de la valeur à l'organisation, en planifiant selon les risques, en communiquant efficacement et en allouant adéquatement les ressources.
- Norme 2100 « Nature du travail » : L'audit interne doit évaluer de manière systématique et méthodique les processus de gestion des risques, de contrôle et de gouvernance d'entreprise, contribuant ainsi à leur amélioration.
- Norme 2200 « Planification de la mission » : Les auditeurs internes doivent élaborer un programme détaillé pour chaque mission, précisant les objectifs, la durée et les ressources allouées.
- Norme 2300 « Accomplissement de la mission » : Les auditeurs internes doivent collecter, analyser, évaluer et documenter les informations nécessaires pour atteindre les objectifs de la mission, en se basant sur des analyses appropriées.
- Norme 2400 « Communication des résultats » : Les auditeurs internes doivent communiquer les résultats de manière précise, objective, claire, concise, constructive et en temps opportun, incluant les conclusions, les recommandations et les plans d'action.
- Norme 2500 « Surveillance des actions de progrès » : Le responsable de l'audit interne doit mettre en place un processus de suivi pour garantir que les mesures sont effectivement mises en œuvre par la direction ou que la direction générale accepte le risque de ne rien faire.

- Norme 2600 « Acceptation des risques par la direction générale » : En cas d'estimation d'un risque résiduel potentiellement inacceptable, le responsable de l'audit interne doit examiner la question avec la direction générale et la soumettre au Conseil si nécessaire pour résolution.

1.2.3. Phases d'une mission d'audit interne :

L'IFACI propose une méthodologie en plusieurs étapes pour la conduite d'une mission d'audit interne :

- Définir les objectifs et le périmètre de la mission.
- Tenir une réunion d'ouverture pour démarrer officiellement la mission.
- Analyser les processus et leurs objectifs.
- Identifier et évaluer les risques.
- Évaluer la conception du dispositif de contrôle.
- Valider le référentiel d'audit avec les audités.
- Sélectionner les objectifs d'audit.
- Élaborer le programme de travail.
- Ajuster le budget et allouer les ressources.
- Valider l'organisation de la mission.
- Conduire la réunion de lancement de la phase d'accomplissement.
- Collecter les informations et constituer les preuves d'audit.
- Valider les preuves d'audit avec les audités.
- Analyser les causes des lacunes et formuler des recommandations.
- Conduire la réunion de clôture pour valider les observations.
- Finaliser le plan d'actions pour la mise en œuvre des mesures correctives.
- Rédiger le rapport d'audit.
- Valider le rapport avant sa diffusion.

Pour la documentation utilisée lors d'une mission d'audit, l'IFACI énumère les documents suivants :

- **Lettre de mission** : Définit les objectifs et le périmètre de la mission.
- **Programme de travail** : Organise les étapes de la mission et les objectifs d'audit.
- **Fiche de test :** Utilisée pour collecter des informations et des preuves, ainsi que pour valider ces preuves.

- **Fiche d'observation :** Employée lors de l'analyse des causes et de l'élaboration des recommandations.
- **Rapport d'audit :** Résume les résultats de la mission et les conclusions, rédigé et validé à la fin de la mission.
- **Fiche de suivi de mission :** Document utilisé tout au long de la mission pour suivre les étapes et les actions.

1.2.4. Outils de l'audit interne :

Voici les outils utilisés dans la même fiche méthodologique de l'IFACI pour guider une mission d'audit interne :

- **Entretien :** Utilisé pour collecter des informations et comprendre les activités du domaine audité, ainsi que pour rassembler des preuves d'audit.
- **Grille d'analyse des tâches :** Permet de visualiser les responsabilités des personnes ou services afin de détecter les incohérences dans la répartition des tâches.
- **Diagramme de flux :** Représente visuellement le déroulement d'un processus pour faciliter la compréhension et l'analyse des contrôles internes.
- **Approche Processus :** Méthode pour décrire systématiquement les activités du domaine audité, identifiant leurs objectifs, leurs risques et les contrôles associés.
- **Test de cheminement :** Permet de suivre en détail les différentes étapes d'une opération en impliquant les parties prenantes concernées.
- **Hiérarchisation des risques :** Aide à sélectionner les risques à évaluer pour définir le périmètre des travaux d'audit.
- **Référentiel d'audit :** Répertorie les objectifs et risques de chaque processus de l'entité auditée ainsi que les contrôles associés.
- **Diagramme Cause / Effet :** Structure les réflexions lors de l'analyse des causes des dysfonctionnements constatés.
- **Questionnaire de Contrôle Interne** : Guide le questionnement pour évaluer les dispositifs de contrôle.
- **Brainstorming :** Favorise la génération d'idées pour résoudre un problème donné.
- **Piste d'audit :** Permet de retracer l'origine d'une opération pour une compréhension approfondie.

- **Circulation :** Obtention de preuves fiables en demandant une vérification à un tiers externe à l'organisation.
- **Procédure d'audit analytique :** Fournit des preuves précises pour identifier les éléments nécessitant des procédures d'audit supplémentaires.
- **Observation :** Obtention de preuves directes d'une situation.
- **Echantillonnage statistique :** Permet d'extrapoler les observations effectuées sur un échantillon à l'ensemble de la population.
- **CAATs (Computerized Assisted Audit Tools) :** Outils informatiques pour extraire et analyser des données volumineuses.

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

L'audit interne vise à évaluer le processus ERM, qui peut varier selon divers facteurs organisationnels. Peu importe sa forme, l'audit doit garantir la couverture des risques significatifs. Le professeur Mashal a examiné le rôle de l'audit interne dans la gestion des risques, en abordant deux perspectives distinctes.

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

La gestion des risques comprend quatre phases principales : l'identification et l'évaluation des risques, la hiérarchisation et la planification des réponses aux risques, ainsi que la surveillance, qui repose sur l'audit interne conformément aux normes comme l'IRM 2002 et le COSO ERM 2017.

L'Institute of Risk Management (IRM, 2002) énumère divers rôles de l'audit interne dans la gestion des risques, soulignant que ces rôles peuvent varier selon les organisations. Parmi ces rôles, on retrouve :

- Orienter les travaux d'audit interne vers les risques significatifs identifiés par la direction et auditer le processus de gestion des risques de l'organisation.
- Fournir une assurance objective sur la gestion des risques.
- Apporter un soutien actif et participer à l'ERM.
- Faciliter l'identification et l'évaluation des risques, ainsi que former le personnel hiérarchique à la gestion des risques et au contrôle interne.
- Coordonner les rapports sur les risques destinés au conseil d'administration et au comité d'audit.

En déterminant le rôle le plus adapté pour une organisation donnée, l'audit interne doit veiller à respecter les exigences professionnelles d'indépendance et d'objectivité.

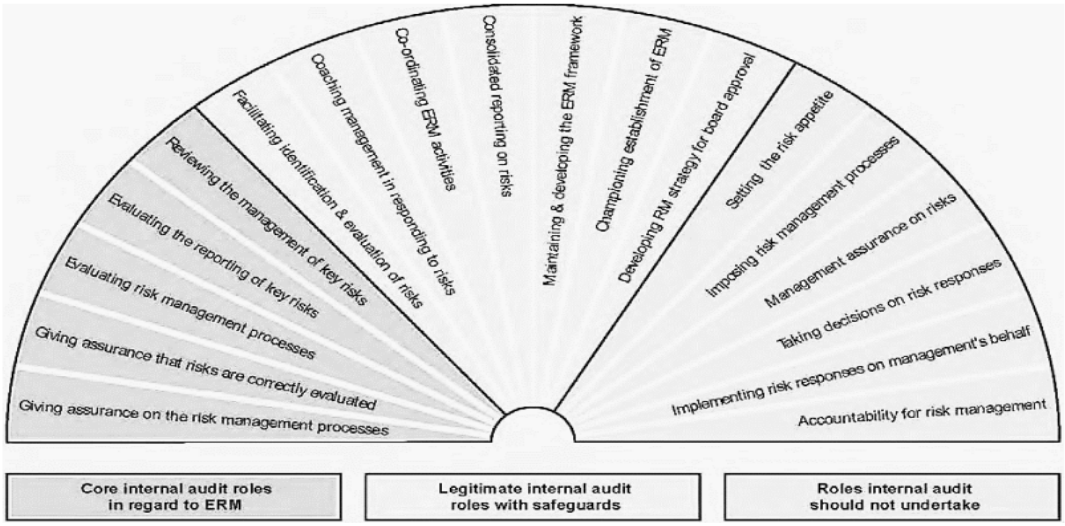
2.2. Le rôle de l'AI dans l'ERM selon les normes IIA :

L'audit interne doit évaluer l'efficacité des processus de gestion des risques et contribuer à les améliorer, comme stipulé par les normes de l'IIA (2120, 2017, p. 20). Une enquête menée par l'IIA auprès de plusieurs entreprises a montré que l'audit interne joue un rôle crucial dans la gestion des risques, étant considéré comme la troisième ligne de défense après le conseil d'administration. Son rôle principal est d'évaluer et d'améliorer l'efficacité du processus de gestion des risques, en fournissant des conseils et une assurance objectifs à la direction générale et au conseil d'administration, ainsi qu'en assurant le maintien des principaux risques à un niveau acceptable (Kertali et Tahajuddiny, 2018).

Après la publication du cadre COSO ERM, l'Institut des auditeurs internes a émis une prise de position, clarifiant le rôle de l'audit interne dans la gestion des risques. Selon les sections révisées en 2017, l'IIA définit l'audit interne comme une fonction indépendante au sein d'une organisation, chargée d'évaluer les activités et de fournir assurance et conseils dans les domaines de la gestion des risques, du contrôle et de la gouvernance. Cela inclut l'assurance que les risques sont correctement évalués en examinant les processus de gestion des risques ainsi que le reporting et la gestion des principaux risques.

Selon ce même document, le rôle de l'audit interne a été classifié en trois types résumés dans la figure en éventail suivante :

La figure (11) : présente le rôle de l'audit interne dans la gestion des risques d'entreprise, tirée du document "IIA Position Paper : The Role Of Internal Auditing In Enterprise-Wide Risk Management"



Source : publié par l'IIA en 2009, page 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 présenter dans le tableau qui suit :

Tableau(05) : Le rôle de l'audit interne dans l'ERM, inspiré de «IIA position paper : the role

Typologies des rôles de l'audit interne dans l'ERM	
Principaux rôles de l'audit interne dans le	- Donner une assurance sur les processus de gestion des risques ; - Donner l'assurance que les risques sont bien évalués ;
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.

of internal auditing in enterprise-wide risk management»,

Source : 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 jouer un rôle crucial au sein des organisations qui ne disposent pas de système de gestion des risques d'entreprise (ERM). Dans de telles circonstances, les missions de l'audit interne varient :

- Sensibiliser aux risques et à l'importance du contrôle interne ;
- Encourager l'adoption de l'ERM en persuadant la direction générale de mettre en place un processus de gestion des risques structuré ;
- Assister l'entreprise dans l'identification et l'évaluation des risques en menant des entretiens avec les principaux responsables, pour évaluer l'impact, la probabilité d'occurrence et le niveau de maîtrise des risques ;

Les auditeurs internes jouent un rôle crucial dans la coordination et la gestion des risques en participant aux comités des risques et aux activités de suivi. Leur responsabilité est d'identifier et d'auditer tous les risques significatifs pour le conseil d'administration et la direction, élargissant ainsi leur fonction à un audit basé sur les risques. Ils évaluent le processus de gestion des risques pour garantir une définition adéquate des dispositifs de contrôle interne. Cependant, la décision finale sur leur rôle dans ce processus appartient à la direction générale et au conseil d'administration, qui doivent tenir compte de la culture organisationnelle, des compétences de l'équipe d'audit interne et de l'environnement local. Ces questions doivent être discutées en profondeur et approuvées par le conseil d'administration pour préserver l'indépendance de l'audit interne.

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

Les normes IIA précisent que l'évaluation du processus de gestion des risques est cruciale, conférant ainsi aux auditeurs internes une grande responsabilité dans cette démarche. L'audit interne est vital pour toute organisation afin d'atteindre ses objectifs stratégiques et opérationnels, en assurant une gestion adéquate des risques. Cela implique l'identification, l'évaluation et le traitement des risques significatifs de manière appropriée et en accord avec

l'appétence au risque de l'organisation. Une communication efficace des risques entre les membres du management et du conseil d'administration est également essentielle. (E.Sallou, 2019)

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

- Être basé sur des données réelles pour identifier les tendances et indicateurs de risque.
- Être dynamique et réactif aux événements externes et aux évolutions des risques.
- Fournir constamment des informations pertinentes en temps réel.
- Prendre en compte de manière exhaustive toutes les formes et impacts des risques.
- Collaborer pour assurer le fonctionnement harmonieux des trois lignes de défense.
- Être orienté vers l'avenir en fournissant des notifications sur les événements passés, futurs et les actions requises.
- Tenir compte du contexte en fournissant des informations pertinentes aux responsables à différents niveaux et fonctions, tout en étant aligné sur les objectifs généraux de l'entreprise.
- Être hautement efficace et géré par une technologie spécifiquement conçue pour répondre à ces exigences.

Pour une gestion efficace des risques, il est essentiel de suivre un processus de management conforme aux normes établies. Cela inclut l'audit régulier du processus pour garantir sa conformité et évaluer sa performance en vue d'améliorations. Étant donné la dynamique des organisations et de leur environnement, une surveillance continue des processus de gestion des risques est nécessaire, utilisant diverses méthodes et outils d'évaluation.

3.1. Approche par principe clés :

Selon Sallou (2019), pour être pleinement efficace, tout processus de management des risques doit respecter les caractéristiques ou principes minimum requis par le cadre de référence adopté. Dans notre cas, nous évaluerons 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 :

- **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 des résultats qui peuvent être comparés.
- **Adapté :** Le processus de gestion des risques est adapté au contexte spécifique de l'organisation et à ses objectifs.
- **Inclusif :** Les parties prenantes sont impliquées de manière opportune, ce qui permet de prendre en compte leurs connaissances et leurs perspectives.
- **Dynamique :** Le management des risques est réactif aux changements dans l'environnement interne et externe de l'organisation.
- **Utilisation de l'information :** Les décisions sont basées sur des données historiques, actuelles et futures, en tenant compte des limites et incertitudes.
- **Facteurs humains et culturels :** Les comportements et la culture organisationnelle ont un impact significatif sur la gestion des risques.
- **Amélioration continue :** Le processus de gestion des risques est constamment amélioré grâce à l'apprentissage et à l'expérience.

Figure(12) : Principes de la norme ISO 31000, tirés de « ISO 31000:2018 (Fr) Management du risque – Lignes directrices Risk management – Guidelines ». ISO.

Source : 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 une série d'activités interconnectées qui transforment des entrées en sorties. Ces processus sont généralement planifiés et mis en œuvre dans des conditions contrôlées afin d'apporter de la valeur ajoutée. Cette approche, faisant partie des sept principes de la démarche qualité de la norme ISO 9001:2015, est directement liée aux idées clés de la norme ISO 31000. L'approche processus permet de décrire une organisation en identifiant les processus qui regroupent ses principales activités telles que la direction, la finance, les opérations, etc. Son utilisation conduit à des résultats plus efficaces et efficients.

Il peut exister plusieurs processus opérationnels qui se déroulent simultanément. La première étape de l'approche par processus consiste à déterminer tous les processus de l'organisme. Ces processus, représentés par une cartographie, sont de trois types :

Tableau(06) : Types de processus pour une approche processus complète, inspiré de « AXESS QUALITE – l'approche processus ».

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.

Source : http://www.axess-qualite.fr/approche-processus.html

Pour le processus de gestion des risques (ERM), l'adoption de cette approche vise à évaluer la présence, la pertinence et la conformité de chaque étape par rapport au référentiel choisi, tel que l'ISO 31000, composé de cinq phases, comme expliqué précédemment. Pour ce faire, nous recueillerons des preuves d'audit en répondant à un questionnaire après avoir instauré l'approche processus dans l'organisation, identifié le processus à auditer ainsi que ses activités sensibles et les risques associés. L'absence de certaines composantes indique souvent une inefficacité du management des risques. Ci-dessous, des exemples de questions permettant de vérifier certains aspects des différentes phases du processus ERM (E.Sallou, 2019).

- **Communication et consultation :** Les échanges avec les parties prenantes et au sein du secteur d'activité sont-ils structurés et réguliers ?

- **Etablissement du contexte :** Les responsables de la gestion des risques comprennent-ils bien l'environnement externe et interne ainsi que les activités de l'organisation pour identifier tous les risques de manière formelle et structurée ?

- **Appréciation du risque :** L'organisation évalue-t-elle les risques de manière à les classer par ordre d'importance relative pour établir les priorités de traitement ?

- **Traitement du risque :** Les décisions sur le traitement des risques sont-elles prises de manière rationnelle ?

- **Surveillance et revue :** Un suivi des plans de traitement des risques est-il effectué, incluant la surveillance de l'efficacité des contrôles et l'évitement des activités interdites ? L'évolution du contexte a-t-elle un impact sur les risques ?

3.3. Approche par modèle de maturité :

Pour contrôler la complexité et les risques organisationnels, il est crucial de maîtriser les fonctions et services essentiels. L'amélioration efficace des processus est ainsi primordiale pour parvenir à cette maîtrise.

L'évaluation selon l'approche du "modèle de maturité" du processus ERM permet une analyse continue et une amélioration de la performance et de la qualité de l'ERM. Plusieurs modèles de maturité ont été développés par différents référentiels tels que la norme ISO/SPICE, la norme ISO 9004:2018, CMM, etc. Quel que soit le référentiel choisi, la maturité est généralement définie sur cinq niveaux.

La mise en œuvre de cette approche nécessite une définition préalable :

- Définir des règles de fonctionnement basées sur une liste d'exigences détaillées pour mesurer les progrès réalisés.
- Fournir un guide pratique pour respecter les règles et les exigences associées, tout en mesurant les performances réelles par rapport à chacune d'elles.
- Utiliser des outils capables d'enregistrer les performances et les progrès, tout en les soumettant à des vérifications périodiques effectuées par la direction.

Le modèle CMMI (Capability Maturity Model Integration), élaboré par le SEI (Software Engineering Institute) de l'Université Carnegie Mellon, est largement utilisé pour évaluer et améliorer la maîtrise des processus techniques et managériaux. Structuré en cinq niveaux, il permet d'évaluer la maturité d'un processus et de le faire évoluer vers un niveau supérieur en identifiant les critères à satisfaire à chaque étape de progression.

Tableau (07) : Les niveaux de maturité du CMMI, réalisé par nous-même, inspiré de « Management de la qualité pour la maîtrise du SI »

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.

Source : A. Carlier, 2006, p. 182, LAVOISIER.

CONCLUSION DU DEUXIÈME CHAPITRE :

Le but de ce chapitre était d'explorer un processus de gestion des risques et de mettre en évidence le rôle crucial de l'audit interne dans son amélioration. Pour ce faire, nous avons divisé notre travail en trois sections.

Dans la première, nous avons présenté un exemple de processus de gestion des risques basé sur la norme ISO 31000 "Management des risques". Cela nous a permis de comprendre que l'adoption d'un cadre complet de gestion des risques, accompagné d'un processus ERM conforme aux normes, améliore le reporting des risques et facilite l'identification des principaux risques susceptibles d'impact sur l'organisation. De plus, cela peut améliorer la productivité et la conformité.

Dans la deuxième section, nous avons exploré la relation entre le contrôle interne et un processus ERM. Nous avons souligné l'importance de combiner ces deux fonctions pour une

meilleure gestion, minimisation, voire élimination des risques, afin de garantir la sécurité et la continuité des activités de l'entreprise.

Enfin, dans la troisième section, nous avons abordé l'importance de l'évaluation du processus ERM par l'audit interne. Cette évaluation aide les organisations à améliorer l'efficacité de leurs processus de gestion des risques. En effet, le rôle principal de l'audit interne est de fournir une assurance à la direction et au conseil sur la gestion des risques, ainsi que sur l'efficacité du processus ERM.

L'ERM est un processus structuré, cohérent et continu, appliqué à l'ensemble de l'organisation. Correctement mis en œuvre, il permet d'identifier et d'évaluer les risques, de décider des réponses à apporter aux opportunités et menaces affectant la réalisation des objectifs, et d'en rendre compte. C'est pourquoi l'IIA met l'accent sur l'implication de l'audit interne dans la gestion des risques, et surtout dans l'amélioration des processus concernés.

CHAPITRE III

EVALUATION DU PROCESSUS DE MANAGEMENT DES RISQUES AU SEIN DE LA B.N.A.

CHAPITRE III : EVALUATION DU PROCESSUS DE MANAGEMENT DES RISQUES, CAS DE LA B.N.A.

Les deux premiers chapitres de notre travail ont exploré la dimension théorique, nous permettant d'aborder la notion de système d'information et son rôle crucial dans une organisation. Nous avons également souligné l'importance de gérer les risques opérationnels associés à un SI pour garantir sa sécurité et son bon fonctionnement. Dans le deuxième chapitre, nous avons mis en avant l'importance d'un processus de gestion des risques conforme aux normes, soulignant le rôle clé de l'audit interne dans cette démarche. Pour valider nos hypothèses et répondre à nos questions secondaires, nous avons collecté des données auprès de la Banque Nationale d'Algérie (B.N.A). Dans ce troisième chapitre, nous présenterons la B.N.A, ses activités d'audit interne et de gestion des risques. Ensuite, après avoir exposé notre méthodologie, nous analyserons les données collectées pour en tirer des conclusions et potentiellement répondre à notre problématique.

SECTION 1 : PRESENTATION DE LA BANQUE NATIONALE D'ALGERIE B.N.A.

Dans cette section, nous nous concentrons sur la présentation de la Banque Nationale d'Algérie (BNA) et de ses divers départements concernés. Nous avons débuté par une présentation générale de la BNA, puis nous avons examiné en détail les missions et la structure de la Direction de l'Audit Interne de la banque. De plus, nous avons décrit et étudié l'organisation de la gestion des risques au sein de l'institution bancaire.

1. Historique de la BNA :

Fondée le 13 juin 1966, la Banque Nationale d'Algérie (BNA) constitue la première banque commerciale en Algérie, résultant de la fusion des activités algériennes du Crédit Foncier d'Algérie et de Tunisie. Ayant un capital de 150 milliards de dinars algériens, son siège social se situe à Alger, au 8 boulevard Che Guevara. En septembre 1995, la BNA a été pionnière en obtenant l'agrément conformément à la loi 90-10 relative à la Monnaie et au Crédit, lui permettant d'exercer toutes les activités d'une banque universelle et de financer l'agriculture.

En 2013, la BNA a annoncé un bénéfice net de 30,2 milliards de dinars algériens, et en juin 2018, son capital est passé de 41,6 milliards à 150 milliards de dinars algériens. Avec plus de 2 513 197 comptes clients en 2015, la BNA dispose d'un réseau de 43 agences réparties sur tout le territoire algérien, comprenant 6 directions de réseau d'exploitation et de distributeurs automatiques de billets, ainsi que 90 guichets automatiques de banque. Son effectif compte également plus de 5 000 collaborateurs.

La BNA a étendu son réseau en mettant à la disposition de sa clientèle 235 agences, implantées sur l'ensemble du territoire national, supervisées par 21 Directions régionales. Dans le cadre du développement de la monétique, la BNA délivre gratuitement des cartes CIB à ses clients, facilitant ainsi la réalisation de leurs opérations quotidiennes à travers ses 100 Guichets Automatiques de Banque et 174 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 :

- 235 agences réparties sur tout le territoire national.
- 21 Directions de Réseau d'Exploitation.
- 174 Distributeurs Automatiques de Billets.
- 100 Guichets Automatiques de Banque.
- Plus de 5000 collaborateurs.
- Plusieurs centaines d'entreprises abonnées au service.
- 543772 Cartes InterBancaires.
- 2 639 319Comptes Clientèles.
- 88805 Clients Abonnés en E-Banking.
- Plus de 5 221 Terminaux de Paiement Électronique installés.
- 64 webmarchands.

1.2.Structure organisationnelle de la BNA :

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	- Direction de L'Encadrement du réseau.	La division gestion des moyens	- Direction des Ressources Humaines et Direction de la
			- 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

Source : www.bna.dz.

1.3.Missions et services de la BNA :

De façon générale, les banques ont pour objectif de recevoir les dépôts du public, de collecter l'épargne, de fournir et de gérer les moyens de paiement, ainsi que d'accorder des prêts. Dans cette optique, la B.N.A offre à sa clientèle une large gamme de produits et services bancaires, ainsi que des solutions d'assurance, afin de répondre à tous leurs besoins.

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.

Tableau (09) : Les différents produits et services de la B.N.A

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.	

Source : www.bna.dz.

2. Présentation de la fonction interne de la BNA :

La fonction d'audit interne au sein de la BNA a été établie le 26 février 1995 sous la forme d'une cellule rattachée à l'inspection générale sur le plan hiérarchique et administratif. Ses missions et son organisation ont été définies le 23 novembre 1995 par le biais d'une circulaire. Le 28 décembre 2006, elle a évolué pour devenir une direction directement rattachée au président directeur général, lui conférant ainsi les prérogatives et les pouvoirs nécessaires pour mener à bien ses missions. La charte d'audit de la BNA, qui englobe l'ensemble des activités et des fonctions de la DAI, stipule que l'audit interne est un dispositif permanent et indépendant chargé d'évaluer l'efficacité du système de contrôle interne ainsi que de l'ensemble des processus.

2.1. Missions de la DAI :

La Banque Nationale d'Algérie a défini, à travers une circulaire interne, les missions de sa direction de l'audit interne. Voici les principales missions :

- Renforcer et protéger la valeur de la banque en offrant des assurances, des conseils et des points de vue objectifs basés sur une approche axée sur les risques.
- Évaluer de manière systématique et méthodique la qualité du système de contrôle interne et des processus de gestion des risques.
- Formuler des recommandations appropriées, reconnues pour leur valeur ajoutée, visant à améliorer le système de contrôle interne.
- Communiquer les résultats de ses missions à la Direction Générale, au Comité d'Audit et aux parties prenantes concernées.
- Assurer le suivi de la mise en œuvre effective des recommandations formulées.

2.2. Organisation de la DAI :

La DAI est structurée en équipes comprenant des Auditeurs Seniors, des Auditeurs et des Auditeurs Juniors, accompagnés d'un service de "Gestion Administrative", sous la direction d'un directeur.

2.2.1. Le directeur d'audit interne :

Sous son mandat, le directeur de l'audit interne à l'autorité de diriger, coordonner et assigner les tâches, les fonctions, les activités et les missions au sein de la structure dont il est responsable. Il est chargé de concevoir et de mettre en œuvre les plans d'action et les rapports d'activité de la direction, en conformité avec le plan d'action préalablement approuvé par la direction générale et en respectant les prérogatives et règlements en vigueur. Il veille également à la formation du personnel sous sa direction.

Parmi ses rôles et responsabilités, on trouve :

- Élaborer les méthodes de travail de la direction.
- Assurer le suivi de l'exécution des missions d'audit prévues.
- Valider les missions menées par les auditeurs.
- Présenter les rapports et les synthèses des missions effectuées à la Direction Générale.

- Rendre compte au Comité d'Audit de l'avancement du plan d'action à la fin de chaque semestre.
- Fournir, sur demande du Comité d'Audit, des éclaircissements et des détails pertinents concernant le programme annuel et les rapports d'audit.
- Superviser la mise en œuvre des recommandations découlant des missions d'audit.
- Participer aux missions d'audit stratégiques ou aux dossiers spécifiques.

2.2.2. Auditeurs et auditeurs seniors :

L'Auditeur Senior a pour responsabilité de superviser, d'animer et de suivre les travaux des missions qui lui sont confiées, en veillant à leur achèvement dans les délais impartis. Il assure également le lien avec le responsable de la DAI et les parties auditées. Ses principales fonctions incluent :

- Participer à la préparation et à la planification des missions.
- Répartir les tâches entre les membres de l'équipe d'audit.
- Surveiller l'avancement des travaux.
- Valider les résultats obtenus par les auditeurs.
- Rédiger les comptes rendus de mission, les rapports finaux et les synthèses correspondantes.
- Assurer le suivi des recommandations émises.
- Contribuer à l'élaboration du plan d'action et des rapports périodiques.
- Participer à l'enrichissement des projets de textes organiques soumis à la DAI.

Quant à l'Auditeur, son rôle consiste à participer aux missions d'audit pour évaluer les risques et l'efficacité des dispositifs de contrôle. Il exécute les tâches qui lui sont assignées par le chef de mission et collabore avec l'Auditeur Senior. En ce qui concerne l'Auditeur Junior, il apporte sa contribution aux travaux de l'équipe d'audit.

2.2.3. Le service gestion administrative :

D'après les documents internes de la BNA, le service a pour mission principale d'assurer la gestion des ressources humaines et matérielles de la direction, ainsi que de la cellule Audit de conformité charia. Le chef de service a les responsabilités suivantes :

- Assurer le respect du règlement intérieur de la banque et veiller à la discipline générale.
- Gérer les dossiers administratifs du personnel.
- Suivre les programmes de formation mis en place pour le personnel.
- Élaborer et suivre le planning des congés du personnel.
- Contrôler et approuver les relevés de frais de mission du personnel.
- Élaborer le budget et assurer un suivi régulier des réalisations budgétaires.
- Effectuer les commandes de fournitures et de consommables et superviser les livraisons.
- Gérer l'économat.
- Garantir l'exactitude des écritures comptables.
- Finaliser la journée comptable et produire les différents états financiers.
- Superviser et mettre à jour les fichiers d'inventaire physique du matériel et du mobilier de la DAI ainsi que de la cellule Audit de Conformité, et concilier les inventaires physiques avec les services concernés de la banque.
- Gérer les abonnements et régler les factures (redevances, consommations, etc.).
- Tenir à jour les registres légaux.
- Assurer la logistique et régler les frais liés à l'organisation des réunions du Comité d'Audit.

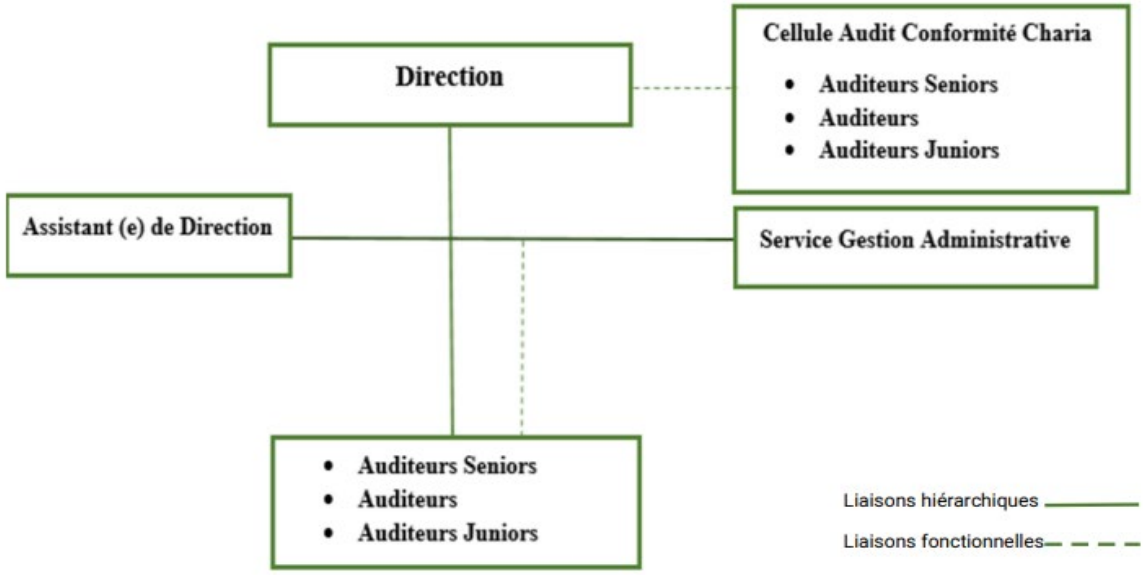


Figure (13) : L'organigramme de la Direction d'Audit Interne de la B.N.A

Source : la documentation interne de la BNA.

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

L'audit interne de la banque couvre l'ensemble de ses activités et fonctions conformément à la politique générale établie par l'organe dirigeant. Selon la circulaire interne de la banque, l'audit interne est une activité indépendante et objective qui fournit à l'organisation une assurance sur le degré de maîtrise de ses opérations, offre des conseils pour les améliorer et contribue à créer de la valeur ajoutée. Il aide l'organisation à atteindre ses objectifs en évaluant de manière systématique et méthodique ses processus de gestion des risques, de contrôle et de gouvernance, tout en proposant des mesures pour renforcer leur efficacité.

La DAI dispose des prérogatives et des pouvoirs nécessaires pour mener à bien ses missions, comme le précise sa circulaire interne. La nature des interventions de l'audit interne est définie comme suit :

- **Audit d'efficacité :** Il vise à examiner la qualité et la pertinence des procédures mises en place pour assurer la conformité aux lois, règlements et politiques de la banque.

- **Audit opérationnel :** Il implique l'évaluation de la qualité et de la pertinence des systèmes et des procédures, ainsi que l'adéquation des ressources et des méthodes aux objectifs définis, tout en analysant de manière critique les structures et l'organisation.

- **Audit des procédures :** Son objectif est de vérifier l'application et l'efficacité des procédures, notamment en matière de gestion des risques.

- **Audit comptable et financier :** Il se concentre sur la vérification de l'exactitude et de la fiabilité des procédures comptables, des enregistrements comptables et des états financiers.

- **Audit des systèmes d'informations :** Il concerne le contrôle des systèmes d'information et comptables.

- **Audit réglementaire :** Son rôle est de vérifier la conformité des dispositifs en place aux exigences légales et réglementaires, ainsi que l'exactitude, la fiabilité et l'opportunité des rapports réglementaires.

- **Audit de management :** Il évalue la qualité de l'approche en matière de gestion des risques et de contrôle interne par les responsables, conformément aux objectifs de la banque.

La Direction d 'Audit Interne relève directement de l'autorité du Directeur Général et est supervisée par un directeur ayant une relation hiérarchique avec lui. Selon les documents internes de la banque, son domaine d'intervention englobe l'ensemble des structures de la banque avec lesquelles elle entretient des relations fonctionnelles et de collaboration, notamment :

- Le Comité d'Audit (CA)
- L'Inspection Générale
- La Division Risque 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)

De plus, la Direction d'Audit Interne est en relation avec divers partenaires externes ainsi qu'avec les commissaires aux comptes.

4. La division risque et contrôle permanent :

Placée sous la direction directe du directeur général, la Division Risques et Contrôle Permanent occupe une position hiérarchique et de coordination au sein de la Direction du Contrôle Permanent (DCP), de la Direction de la Gestion des Risques (DGR), et de la Cellule Sécurité des Systèmes d'Information.

Établie et mise en œuvre le 23 septembre 2019, en conformité avec les exigences réglementaires de la loi 11-08 de la Banque d'Algérie concernant le contrôle interne des banques et établissements financiers, la DRCP exerce une autorité fonctionnelle sur l'ensemble des structures de la banque dans son domaine d'activité. (Documents internes de la BNA, 2024)

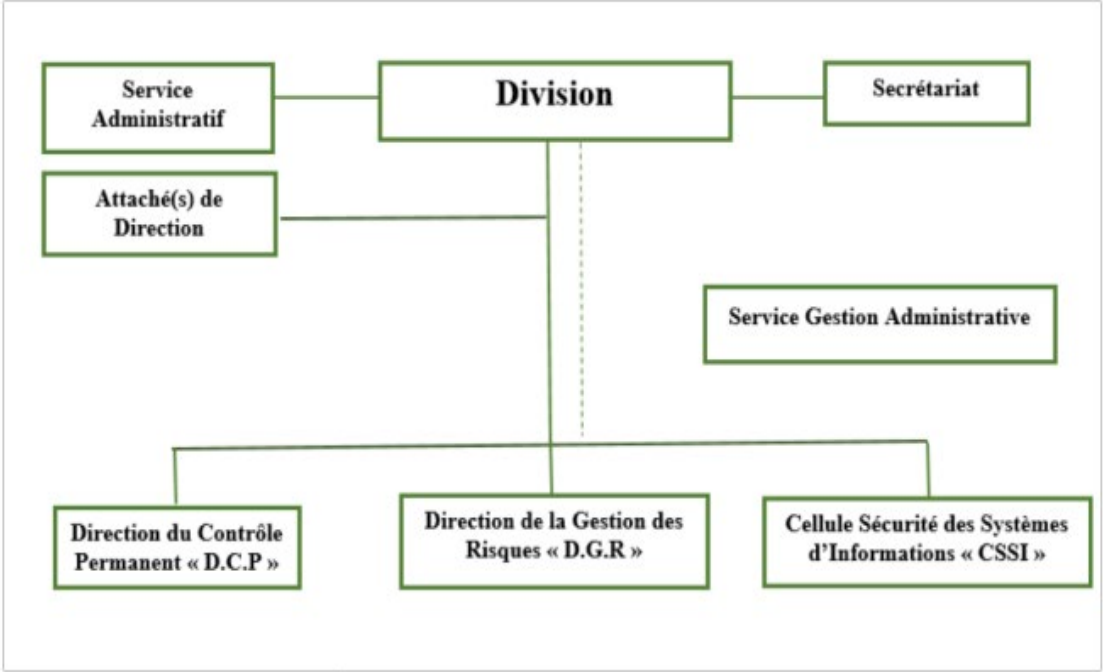
3.1.Organisation de la DRCP :

La Direction des Ressources et de la Coopération de Proximité (DRCP) se structure de la manière suivante pour garantir l'accomplissement de ses missions :

- **Le responsable de la division :** Il est chargé de la gestion hiérarchique de la division et rend compte de ses activités au directeur général. Son rôle consiste à élaborer les plans d'action et les budgets de la division, à coordonner les structures sous son autorité et à superviser les dispositifs de contrôle.
- **Les collaborateurs de direction** : Leur mission est d'analyser les dossiers qui leur sont confiés et de consolider les plans d'action des structures rattachées à la division, en tenant compte des objectifs fixés.
- **Le service administratif :** Il assure le suivi et l'exécution des procédures en vigueur, ainsi que les tâches administratives et comptables liées aux activités de la division. Ce service gère également les dossiers du personnel et tient à jour les informations des structures affiliées.

- **Le secrétariat :** Ce service prend en charge les tâches administratives courantes telles que la gestion des communications, la planification des réunions et la gestion de la correspondance.

Figure(14) : l'organigramme de la division Risque et Contrôle Permanent de la B.N.A



Source : la documentation interne de la banque.

3.2.La direction gestion des risques :

Pour garantir une gestion efficace des risques liés à l'expansion de l'activité bancaire, conforme au règlement Banque d'Algérie n°11-08, il est essentiel de mettre en place une organisation dédiée à la gestion des risques. Cette entité vise à atténuer les risques de crédit, financiers et opérationnels.

La mission principale de la direction de gestion des risques est d'identifier, d'évaluer et de surveiller les risques encourus par la banque. Elle est également chargée des responsabilités suivantes :

- Développer des méthodes et des outils pour maîtriser et couvrir les risques.
- Élaborer des procédures pour gérer les différents types de risques.

- ❖ Suivre de près le respect et l'ajustement des limites de risque en fonction de l'évolution des activités de la banque.
- ❖ Préparer des rapports réguliers sur l'exposition de la banque aux risques et les actions à entreprendre.
- ❖ Mettre à jour régulièrement la cartographie des risques opérationnels et partager les résultats avec les organes de la banque.
- ❖ Mettre à disposition des responsables du contrôle permanent et périodique les données sur les incidents significatifs.
- ❖ Surveiller l'évolution de la qualité du portefeuille de crédit global et informer les organes de la banque des résultats.
- ❖ Analyser les rapports reçus sur les différents risques.
- ❖ Rédiger des rapports semestriels et annuels sur la mesure et la surveillance des risques de la banque, en coordination avec toutes les structures concernées.

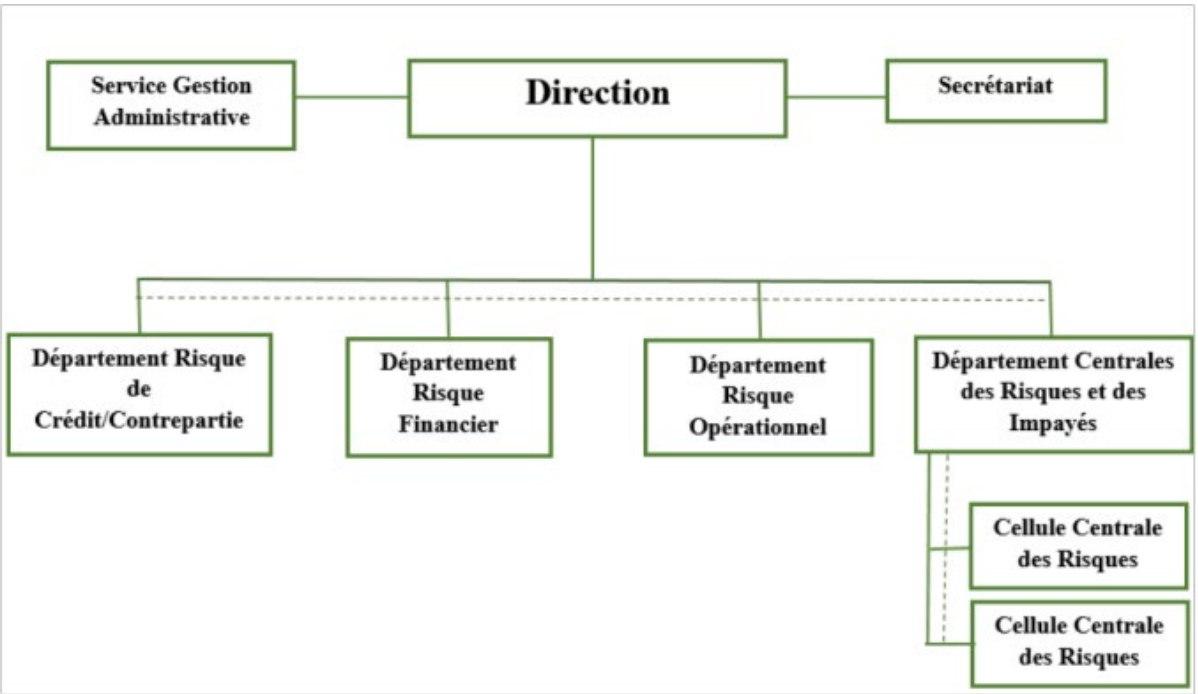
3.2.1. Organisation de la DGR :

La Direction de la Gestion des Risques à la BNA est organisée en quatre départements et un service, comme stipulé dans les documents internes de la banque :

- ➢ **Département Risques de Crédit/Contrepartie :** Sa mission principale est d'assurer la coordination, l'animation et le pilotage de la gestion, de l'analyse et du suivi des risques de crédit.
- ➢ **Département Risques Financiers :** Ce département, dirigé par un chef et des contrôleurs, entretient des liens étroits avec la Direction des Marchés Financiers et la Direction Animation Commerciale. Il est chargé de piloter, animer et coordonner la gestion, l'analyse et le suivi des risques financiers, tels que les risques interbancaires, de liquidité et de taux d'intérêt.
- ➢ **Département Risques Opérationnels :** Son rôle principal est d'assurer la coordination, l'animation et le pilotage de la gestion, de l'analyse et du suivi des risques opérationnels.
- ➢ **Département Centrale des Risques et des Impayés :** Ce département gère la centrale des impayés, avec deux cellules dédiées respectivement aux risques et aux impayés.

- **Service Gestion Administrative :** Sa mission consiste à assurer le suivi et l'exécution rigoureuse, en conformité avec les textes et procédures en vigueur, de toutes les tâches administratives et comptables liées aux activités de la direction.

Figure(15) : organigramme de la Direction Gestion des Risques de la B.N.A



Source : la documentation interne de la banque.

3.3.La cellule sécurité des systèmes d'informations :

Créée conformément à la loi 11-08 de la Banque d'Algérie, la cellule sécurité des systèmes d'information (CSSI) a été établie le 03 Octobre 2019, sous la division des risques et contrôle permanent. Indépendante de la DSI, elle a pour mission de veiller à la sécurité des systèmes d'information de la banque. La CSSI exerce une autorité fonctionnelle sur l'ensemble des structures de la banque dans ce domaine et collabore étroitement avec elles.

3.3.1. Organisation de CSSI :

La cellule, constituée d'ingénieurs en informatique expérimentés, est dirigée par un responsable nommé par le Directeur Général. Ce dernier est chargé de :

- Définir le programme d'activités de la cellule.
- Assurer l'exécution, la coordination et la supervision des travaux.
- Rédiger les rapports semestriels et annuels sur les activités, ainsi que les synthèses à transmettre à la Direction Générale.
- Établir un bilan des interventions effectuées par la cellule.

SECTION 2 : METHODOLOGIE DE L'ETUDE

La revue de littérature a permis de définir le cadre théorique de mon étude, qui servira de base pour élaborer la méthodologie visant à atteindre mes objectifs. Ma prochaine étape consistera à développer le modèle d'analyse et à présenter les outils de collecte et d'analyse des données. Pour mener mon étude à la B.N.A, j'ai utilisé trois outils de collecte et d'analyse des données, étroitement liés entre eux.

1. L'analyse documentaire :

Une approche impliquant l'exploitation des divers documents de la B.N.A, issus de différents sites de travail, est employée pour acquérir une vision globale du fonctionnement de l'entreprise. Les données recueillies par cette analyse seront enrichies par des entretiens.

2. Interviews :

L'interview consiste à questionner une personne sur ses actions, ses idées, etc., afin de recueillir des éléments d'analyse et d'orientation pour mon mémoire. J'ai choisi d'adopter une approche en face-à-face avec les directeurs et responsables pertinents, notamment le directeur de l'audit interne, le directeur de la gestion des risques, la responsable du département des risques opérationnels, la responsable de la division des risques et du contrôle permanent, ainsi que la responsable de la sécurité des systèmes d'information.

3. Le questionnaire :

Le questionnaire représente un outil essentiel pour mener une enquête, permettant de recueillir des informations précieuses sur les activités du répondant. Il est constitué de vingt-sept questions réparties en deux parties : la première se focalise sur le cadre organisationnel de la gestion des risques SI, tandis que la seconde porte sur la compréhension du processus de management des risques. Les questions varient en forme, comprenant des questions fermées à choix unique, des questions fermées à choix multiples et des questions ouvertes.

J'ai utilisé ce questionnaire pour obtenir des renseignements clés qui m'aide à comprendre le fonctionnement de l'organisation, son dispositif de gestion des risques, l'audit interne et sa contribution à ce dispositif.

SECTION 3 : INTERPRETATION DES RESULTATS

Au cours de mon stage à la Banque Nationale d'Algérie, malgré les restrictions de confidentialité et les lacunes en informations, j'ai pu me faire une idée de la fonction de gestion des risques, de la fonction d'audit interne, et de leur impact sur l'amélioration du processus de gestion des risques opérationnels associés aux systèmes d'information.

1. Cadre organisationnel de la gestion des risques SI au sein de la B.N.A :

Sous l'impulsion de l'ancienne direction générale, le concept de risque est une notion relativement récente au sein de l'organisation, tout comme la division Risques et Contrôle Permanent, qui est encore dans une phase embryonnaire. Cependant, cela n'a pas empêché les agents de la BNA, en particulier les opérationnels et les agents de réseaux, de développer 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'est un risque (Article 2, paragraphe i, p. 03), ses différents types, ainsi que l'importance de la mesure et de l'analyse du risque opérationnel (Article 27 de la loi 11.08).

1.1. La fonction gestion des risques de la BNA :

La gestion des risques, en tant qu'objectif majeur de la Direction Générale, occupe une position importante parmi les priorités managériales de l'organisation. Cela s'est matérialisé

par la mise en place d'une division entièrement autonome, ce qui représente une première parmi toutes les banques en Algérie.

1.1.1. Les objectifs de la BNA en gestion des risques :

Ces plans d'actions sont élaborés, actualisés et diffusés sous forme de plans d'action spécifiques à chaque division, direction et cellule. Parmi les mesures prises, on peut citer :

- La conception d'un plan de continuité d'activité actuellement en phase de validation pour atténuer le risque de perturbation du système d'information.
- L'élaboration et la validation en 2021 d'une politique de sécurité des systèmes d'information (PSSI) par la Direction Générale. Cette politique intègre un volet sur la gestion des risques opérationnels liés aux systèmes d'information, mettant en lumière des risques clés tels que la confidentialité et la disponibilité du système d'information.
- La création d'une cellule dédiée à la sécurité des systèmes d'information (CSSI), directement rattachée à la DRCP et indépendante des opérations quotidiennes. Cette initiative permet une surveillance accrue des activités de la DRG et un contrôle approprié. La création de cette cellule répond à l'importance constante accordée à la gestion des risques liés aux systèmes d'information, permettant ainsi l'identification proactive des principaux risques.

La DRCP, étant directement rattachée à la direction générale, dispose des qualifications nécessaires pour exercer une influence significative sur les opérations et les dirigeants.

1.1.2. La définition des responsabilités en la gestion des risques :

La BNA utilise des circulaires spécifiques à chaque division et direction, détaillant les responsabilités de chaque intervenant, qu'il soit directement ou indirectement impliqué dans la gestion des risques. Ces responsabilités sont principalement liées à la gestion de trois risques majeurs : les risques de marché, les risques de crédit et les risques opérationnels. Ces circulaires font l'objet d'améliorations continues, la dernière mise à jour étant celle de la circulaire n°2277 du 15 juillet 2020.

À l'heure actuelle, la direction de la BNA est en train de détailler les procédures relatives à la politique de gestion des risques opérationnels et de la sécurité des systèmes d'information.

1.1.3. Les obligations légales et réglementaires applicables en matière de communication sur les risques :

Au niveau externe, la BNA se conforme aux directives de la Banque d'Algérie en matière de communication sur les risques, comme stipulé dans le règlement n°2014-02 du 16 février 2014 concernant les grands risques et les participations. Ce règlement impose à toutes les institutions financières de :

- Produire un rapport annuel sur la surveillance et la maîtrise des risques, en suivant la méthodologie définie dans ce règlement.
- Déclarer les taux des ratios liés aux risques opérationnels, ainsi que ceux de l'endettement et de la solvabilité, tout en fournissant des scénarios sur les risques de crédit.
- Remplir chaque trimestre des états récapitulatifs fournis par la Banque d'Algérie sur la gestion des risques, tâche gérée par la direction des Reporting Légaux Et Réglementaires (DRLR).

Au niveau interne, la DCP est chargée de produire des rapports semestriels sur le contrôle interne, couvrant les divisions des risques, des engagements, des marchés financiers et comptables.

En outre, la DRCP a institué un comité de sécurité des systèmes d'information (CSSI) afin de diffuser des informations sur les démarches à suivre concernant les risques, et pour assurer une communication avec le comité d'audit.

2. Evaluation des risques liés au SI :

Comme décrit dans la théorie (chapitre 1, section 3, point 3), la Direction des Systèmes d'Information (DSI) est généralement chargée de la gestion des risques liés aux systèmes d'information. Toutefois, pour la BNA, la DSI est simplement une entité de support pour son système d'information. Son rôle se limite à fournir des logiciels et des programmes, en plus du matériel informatique, pour permettre l'exécution de tâches spécifiques telles que la gestion des comptes bancaires avec des logiciels sophistiqués facilitant les virements en ligne et la gestion financière en temps réel.

La DSI fait également appel à un service d'assistance informatique, également connu sous le nom de Help Desk, pour fournir une aide aux utilisateurs sur tous les aspects matériels, logiciels et de mise en réseau. Le Help Desk peut être un service interne ou externe, organisé en groupe ou en fonction organisationnelle, auquel les utilisateurs s'adressent pour résoudre les problèmes informatiques. Il peut être géré par une seule personne prenant les appels ou par une organisation mondiale acceptant les demandes d'assistance en ligne ou en personne, provenant du monde entier.

Souvent, la gestion du service d'assistance est externalisée à des spécialistes qui fournissent une assistance aux utilisateurs au sein de l'entreprise.

2.1. La cellule sécurité des systèmes d'information :

L'évaluation des risques opérationnels liés aux systèmes d'information constitue la mission principale de la CSSI, qui a été créée dans ce dessein. Relevant du responsable de la Sécurité des Systèmes d'Information (SSI), cette mission s'effectue à travers des audits informatiques visant à identifier, évaluer et déterminer les risques associés aux activités informatiques, qu'ils soient opérationnels, financiers ou liés à la réputation.

L'audit informatique, également appelé audit des systèmes d'information ou audit technologique, est réalisé par une entité externe et indépendante au service audité. Son objectif est d'analyser l'organisation informatique, d'identifier les points forts et les points faibles, et de formuler des recommandations pour améliorer la maîtrise des systèmes d'information. Ce processus vise à évaluer les risques des activités informatiques et à les réduire pour renforcer la sécurité des systèmes. (Yende, 2018, p.9)

L'audit informatique se décline en six sous-audits distincts :

- **Audit de la fonction informatique** : qui évalue l'organisation, le pilotage et les relations de la fonction informatique avec les utilisateurs.
- **Audit des études informatiques :** qui examine l'efficacité de l'organisation, de la structure et du pilotage du système d'information.
- **Audit de l'exploitation :** qui s'assure du bon fonctionnement des centres de production informatiques.

- **Audit des projets informatiques :** qui garantit la qualité et la performance des applications développées.
- **Audit d'une application opérationnelle :** qui fournit une assurance sur le bon fonctionnement d'une application spécifique.
- **Audit de la sécurité informatique** : qui évalue le niveau de risque lié à la sécurité informatique et propose des mesures pour renforcer la sécurité des systèmes.

La CSSI réalise régulièrement des audits de sécurité informatique, notamment pour évaluer le niveau de sécurité du système SWIFT, en réponse aux cyberattaques passées. SWIFT, une coopérative internationale fournissant des services de messagerie financière sécurisés, renforce constamment la sécurité de ses échanges, notamment en généralisant l'utilisation de l'authentification à double facteur. Malgré ces mesures, la BNA continue à tester régulièrement la sécurité de son système d'information pour garantir sa robustesse. (Le site de SWIFT, https://www.swift.com)

2.1.1. Teste d'intrusions techniques :

Le Pen-testing, connu également sous le nom de test d'intrusion ou test de pénétration, est une pratique de piratage éthique réalisée par des spécialistes de la sécurité, souvent désignés sous le terme de "White Hats". Son but est d'évaluer la robustesse des mesures de sécurité d'un système informatique en simulant des attaques cybernétiques. Cette démarche permet d'identifier les failles potentielles et d'améliorer la sécurité globale de l'organisation.

Les professionnels de la sécurité utilisent le Pen-testing pour plusieurs objectifs, notamment pour vérifier la conformité réglementaire du système d'information, sensibiliser les employés à la sécurité informatique et évaluer la capacité de l'organisation à détecter et à répondre aux incidents de sécurité.(Imperva,2021)

Il existe plusieurs approches de test de pénétration, dont les plus courantes sont : (contrast Security, s. d.) :

- Les évaluations externes de l'organisation impliquent l'utilisation de procédures réalisées depuis l'extérieur des systèmes de l'organisation, tandis que les tests internes se déroulent dans l'environnement même de l'organisation.

- **Les tests à l'aveugle :** L'objectif est de simuler les actions d'un véritable pirate informatique en utilisant uniquement des informations publiques de l'organisation. Les tests en double aveugle ou ceux où seules quelques personnes au sein de l'organisation sont informées sont également réalisés.
- **Les tests ciblés :** Ces tests impliquent à la fois les équipes informatiques et les équipes de tests d'intrusion, qui sont informées dès le départ de la cible et de la conception du réseau.

Pour effectuer ces tests, une variété d'outils est disponible, notamment sur la plateforme Kali Linux, largement utilisée dans le domaine de la sécurité informatique. Parmi ces outils figurent Nmap pour la collecte d'informations, Lynis pour l'audit de sécurité et la conformité, ainsi que d'autres logiciels spécialisés dans la détection des vulnérabilités et des failles de sécurité.

La responsable de la sécurité des systèmes d'information (RSSI) est chargée de surveiller les indicateurs de sécurité, tels que l'intégrité, la disponibilité et la confidentialité du système. Ces mesures aident à évaluer le niveau de sécurité de l'organisation et à identifier les domaines à améliorer.

2.2.Les missions de la cellule sécurité des systèmes d'informations :

En complément des responsabilités précédemment mentionnées, la circulaire énumère les missions suivantes pour la CSSI :

- Élaborer et actualiser régulièrement le système de management de la sécurité des systèmes d'information de la banque, en conformité avec les objectifs fixés par la direction générale.
- Évaluer et mettre en place un plan de continuité de l'activité informatique en collaboration avec les opérationnels, ainsi que des plans de secours et de sauvegarde informatique.
- Évaluer et mettre en place un processus de gestion des incidents de sécurité des systèmes d'information, ainsi que des procédures et des normes techniques en matière de sécurité informatique.

- Assurer un contrôle permanent du respect des habilitations informatiques et de l'intégration de la sécurité informatique dans les projets.
- Assurer une veille technologique et suivre l'évolution réglementaire en matière de sécurité des systèmes d'information, ainsi que leur mise en œuvre effective.
- Coordonner les investigations avec la direction générale en cas d'incidents de sécurité opérationnelle, et avec la direction de la conformité et du contrôle permanent en cas d'incidents majeurs.
- Mettre en œuvre des actions de formation et de sensibilisation afin de promouvoir et de maintenir une culture de la sécurité des systèmes d'information auprès de l'ensemble des collaborateurs.
- Représenter la banque auprès des organismes externes sur les questions relevant de son domaine d'activité.

2.3.Compétences des auditeurs en matière de SI :

Pour réaliser un audit informatique, il est essentiel de remplir certaines conditions. Cette mission nécessite que les auditeurs soient certifiés en évaluation des systèmes d'information et possèdent une solide expertise en informatique. (Yende, 2018) Actuellement, la BNA s'engage à former ses auditeurs et à les doter des compétences requises pour ce type de mission. À l'heure actuelle, toutes les missions liées à l'évaluation de la sécurité des systèmes d'information face aux risques sont externalisées et confiées à des prestataires étrangers à l'organisation.

Deux principales certifications de référence sont développées par l'ISACA (Information System Audit and Control Association) :

- **La certification CISA (Certified Information System Auditor) :** qui offre la possibilité d'accéder à un module de certification CIA de l'Institute of Internal Auditors (IIA). L'examen se déroule trois fois par an, dans 11 langues différentes et dans 200 villes à travers le monde. Il comporte de 150 à 200 questions à choix multiples, à répondre en 4 heures, couvrant six domaines principaux :

- 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 actifs informatiques.
- Le plan de continuité et le plan de secours informatique.

❖ **La certification CISM (Certified Information Security Manager) :** accordée par l'ISACA, est conçue pour les responsables de la sécurité de l'information. Elle se divise en deux grandes catégories : CRISC (Certifié en Contrôle des Risques et des Systèmes d'Information) et CGEIT (Certifié en Gouvernance des Technologies de l'Information en Entreprise). Le programme de certification CISM couvre cinq domaines clés de la sécurité de l'information :

- La gouvernance de la sécurité de l'information.
- La gestion des risques liés à l'information.
- La mise en œuvre 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 :

Auparavant, la DRCP utilisait COSO et CobiT pour la cartographie des processus et des risques à la BNA. Toutefois, avec la création de la cellule spécialisée dans la sécurité des systèmes d'information, la CSSI, une transition vers l'obtention de la certification ISO 27005 est en cours. Cette norme fournit des lignes directrices pour la gestion des risques liés à la sécurité de l'information dans une organisation.

L'ISO 27005 est conçue pour faciliter la mise en œuvre d'une sécurité de l'information basée sur une approche de gestion des risques. Elle s'applique à tous les types d'organisations confrontées à des risques susceptibles de compromettre la sécurité de leurs informations.

Avant de suivre et d'appliquer les directives de l'ISO 27005, il est essentiel de comprendre les concepts, les modèles, les processus et la terminologie décrits dans l'ISO/IEC 27001 et l'ISO/IEC 27002.

Parallèlement, la DRCP étudie et s'efforce également d'obtenir la certification ISO 31000 en gestion des risques. En ce qui concerne les méthodes de gestion des risques en sécurité de

l'information, la CSSI a opté pour la méthode EBIOSE après avoir exploré la méthode MEHARI, comme mentionné dans le chapitre 1, section 3, point 1.3.

2.5.Les risques opérationnels liés au SI de la BNA :

Parmi les multiples risques opérationnels qu'un système d'information peut rencontrer, les risques liés à la cybersécurité sont les plus fréquents au sein de la BNA, notamment les tentatives de phishing. Bien que ce risque ne soit pas classé parmi les risques majeurs, étant donné que la BNA accorde une grande importance à la sécurité de l'information.

La plupart du temps, le système d'information de la BNA est confronté à des risques physiques tels que les coupures de courant dans l'une de ses agences, ou même un site qui tombe en panne lorsqu'il ne respecte pas les normes.

Heureusement, ces risques n'ont jamais eu d'incidence financière sur l'établissement. Ils affectent plutôt l'image de l'organisation, par exemple lorsqu'un client est mécontent de trouver l'une des agences hors service.

3. Le processus de management des risques de la BNA :

À l'heure actuelle, la B.N.A n'a pas encore instauré de processus de gestion des risques, mais ce projet est actuellement en cours. En attendant, elle répond aux risques en élaborant des plans d'action par le biais de la DGR, des plans stratégiques, ainsi que des plans de continuité d'activité et de sécurité des systèmes d'information. Étant donné le caractère confidentiel des données, il nous est impossible de fournir davantage de détails à ce sujet.

CONCLUSION DU TROISIEME CHAPITRE :

Dans ce dernier chapitre, nous avons exploré les pratiques de gestion des risques opérationnels liés au système d'information de la BNA, ainsi que le rôle de la direction d'audit dans le processus d'ERM. Notre étude nous a permis de comprendre les mesures prises par la BNA pour faire face aux risques de son système d'information, et de déterminer si elle dispose d'un processus ERM et le rôle potentiel de la fonction d'audit interne dans ce processus.

Pour cela, nous avons examiné les différentes composantes de l'organisation générale de la BNA et découvert l'existence d'une division entièrement dédiée à la gestion des risques et au

contrôle permanent, la DRCP. Parmi ces composantes, nous avons identifié une cellule spécifiquement dédiée à la sécurité des systèmes d'information.

Ensuite, nous avons analysé la contribution de la fonction d'audit dans la gestion des risques, notamment en ce qui concerne l'élaboration de la cartographie des risques. À la fin de notre travail, nous avons observé que l'environnement de gestion des risques à la BNA est en constante évolution. L'absence temporaire d'un processus ERM conforme aux normes récentes n'a pas empêché la banque de disposer de dispositifs très pointus pour la gestion des risques liés au SI, et de travailler à son amélioration et à la migration vers de nouvelles procédures encore plus performantes.

La fonction d'audit de la BNA reste également engagée dans l'amélioration du contrôle interne et de la gestion des risques.

CONCLUSION GENERALE

CONCLUSION GENERALE

Dans mon mémoire, la problématique abordée concerne le rôle de l'audit interne dans l'amélioration du processus de gestion des risques opérationnels liés aux systèmes d'information. Mon travail est divisé en deux parties étroitement liées.

La première partie, qui présente le cadre théorique, se compose de deux chapitres. Le premier, intitulé "Gestion des risques opérationnels des systèmes d'informations", il ma permis de comprendre que les organisations modernes sont confrontées à une multitude de risques pouvant compromettre leur efficacité opérationnelle et leur conformité réglementaire. Avec l'essor des technologies de l'information, les risques opérationnels, tels que la cybersécurité, sont devenus plus préoccupants, nécessitant des approches efficaces pour les gérer.

C'est là que la gestion des risques entre en jeu. Cette fonction aide les organisations à gérer, minimiser voire éliminer les risques informatiques, y compris en matière de sécurité de l'information, afin de préserver leur sécurité et leur activité.

Le deuxième chapitre, intitulé "Enterprise Risk Management et la fonction d'audit, ma permis de comprendre que, pour faire face à l'augmentation des risques, il est nécessaire de disposer d'outils de maîtrise des risques de plus en plus efficaces, accompagnés d'une culture de management et de contrôle des risques. Le processus ERM permet de planifier, d'organiser, de diriger et de contrôler les activités d'une organisation afin de réduire les coûts opérationnels et d'améliorer les revenus. J’ai également abordé le lien étroit entre la gestion des risques et l'audit interne. Ce dernier peut fournir des services de conseil qui améliorent la gouvernance, notamment 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 la gestion des risques d'entreprise, à condition que cette activité ne compromette pas son indépendance et son objectivité.

En conclusion, le succès de la mise en œuvre d'un processus ERM dépend largement de la stratégie de l'organisation, de la formation adéquate de ses employés à la gestion des risques, et de l'implication de la fonction d'audit interne dans l'établissement et la mise en œuvre de ce processus. Cela permettra aux organisations de mieux faire face à l'évolution du climat économique et de créer un environnement de travail plus conscient, les protégeant ainsi contre les turbulences futures.

BIBLIOGRAPHIE

BIBLIOGRAPHIE :

Ouvrages :

- Laudon, K., & Laudon, J. (2013). Management des systèmes d'information (13ème édition). Paris : Pearson.
- Reix, R., et al. (2016). Système d'information et management (7ème édition). Paris : Vuibert.
- Moisand, D., & Garnier De Labareyre, F. (2009). Cobit. Pour une meilleure gouvernance des systèmes d'information (1ère édition). Paris : Eyrolle.
- Schick, P., et al. (2010). Audit interne et référentiels de risque (1ère édition). Paris : Dunod.
- Darsa, J. D. (2013a). La gestion des risques en entreprise (3ème édition). France : Gereso.
- Jimenez, C., & Merlier, P. (2004). Prévention et gestion des risques opérationnels (1ère édition). France : Revue Banque.

- 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., & Chauvel, A. M. (1980). Gestion de la production et des opérations (1ère édition). Paris : HRW Ltée.
- Deyrieux, A. (2004). Le système d'information, nouvel outil de stratégie (1ère édition). Paris : Maxima.
- Tassin, P. (2005). Systèmes d'information et management de crise (1ère édition). Paris : Lavoisier.
- Luisot, J. P. (2005). Gestion des risques (1ère édition). Paris : AFNOR.
- Desroches, A., et al. (2005). La gestion des risques (3ème édition). Paris : Lavoisier.
- Autorité des Marchés Financiers (AMF). (2010). Les dispositifs de gestion des risques et de contrôle interne, cadre de référence. France : IFACI.

- Verver, J. (2021). 7 étapes à suivre pour bénéficier d'un ERM améliorant vos performances. Galvanize. Lien
- Carlier, A. (2006). Management de la qualité pour la maîtrise du SI (1ère édition). Paris : Lavoisier.
- Bursh, J. G., & Felix, R. S. (1984). Information System Theory and Practice (1st edition). USA : Hamilton Edition.

Articles scientifiques :

- Mayer, N. J., & 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., & 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., & Elouidani, A. (Décembre 2016). La gestion des risques des systèmes d'information dans les organismes publics au Maroc : quels bénéfices à la performance ? Revue Économie, Gestion et Société. (n°8) https://revues.imist.ma/index.php/REGS/article/download
- Kertali, M., & 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
- 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/

Rapports :

- Petsetidi, Soupek et De La Brosse (2016) ont réalisé une révision du Risk Appétit. https://www.eifr.eu/uploads/eventdocs/56f3c65ae750a.pdf
- World Intellectual Property Organization (WIPO) (2016) a publié un rapport d'audit sur la gestion des risques de l'entreprise. https://www.wipo.int/aboutwipo/en/over
- Le rapport CBOK (2015) traite de la navigation des dix principaux risques technologiques. http://www.iia.nl/actualiteit/nieuws/cbok-report-navigating-technologys-top-10-risks

Mémoires :

- CHETOUI Mohammed Fath Eddine, La Gestion des risques opérationnels dans les activités bancaires, École Supérieure de Commerce, 2017/2018
- MOHAND SAIDI Assia et YAHIATENE Saïd , Le Système d'information Bancaire, Mémoire de fin d'études en vue de l'obtention du diplôme de master en sciences financières et comptabilité, promotion 2018, UNIVERSITE MOULOUD MAMMERI TIZI-OUZOU FACULTE DES SCIENCES ECONOMIQUES, COMMERCIALES ET DES SCIENCES DE GESTION DEPARTEMENT DES SCIENCES DE GESTION.
- REMADNIA Hana, le rôle de l'audit interne dans la gestion des risques opérationnels, Mémoire de fin de cycle, École Supérieure de Commerce, 2017/2018.

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%
- ISO. Guide 73, 2009. Management du risque — Vocabulaire https://www.iso.org/obp/ui/#iso:std
- IIA. (2009). IIA position paper : the role of internal auditing in enterprise-wide risk management. https://www.theiia.org/en/content/position-papers/2009/the-roleof
- 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+Ris
- IIA. (2020). Le modèle des trois lignes de l'IIA.
- https://www.theiia.org/globalassets/
- ISO/TC. (2018). Management du risque — Lignes directrices (ISO Standard No.31000 :2018).
- ISO/IEC. (2000). Ingénierie des systèmes et du logiciel — Exigences de qualité des systèmes et du logiciel et évaluation (ISO Standard No.9000 :2000).
- ISO/IEC. (2015). Système de management de la qualité — Principes essentiels et vocabulaire (ISO Standard No.9000 :2015).

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

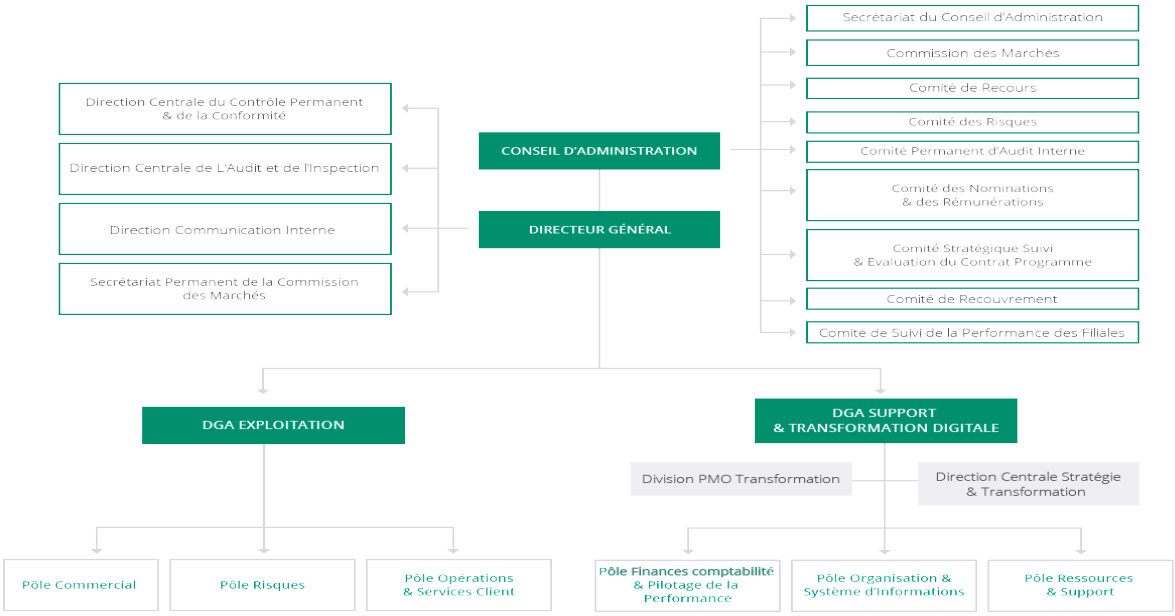
Sites internet :

- Leterme, C. (2020, 14 février). Tout savoir sur la publication d'un article scientifique. Scribbr. Consulté le 02 mars 2024 sur www.scribbr.fr/articlescientifique/publication-article-scientifique
- Caclin, F. (2021). Le risque opérationnel. Fimarkets. Consulté le 13 octobre 2023 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 2023 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 décembre 2023 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 2024 sur http://broadleaf.com.au/old/pdfs/trng_tuts/tut.standard.pdf
- Sallou, E. (2019). Évaluer les processus de management des risques. Consulté le 16 mars 2024 sur https://apprendrelaudit.com/evaluer-les-processus-de-management-des-risques/
- IONOS. (2020). Une gestion des risques normalisée: ISO 31000. Consulté le 2 avril 2024 sur https://www.ionos.fr/startupguide/gestion/iso-31000/
- Certification QSE. (s.d.). Approche processus et Management par approche Système. Consulté le 15 avril 2024 sur https://www.certification-qse.com/approche-processus/
- Takyorian, J. F. (2003). Maturité des processus et amélioration continue. Consulté le 18 avril 2024 sur https://www.infoqualite.fr/maturite-des-processus-et-amelioration continue/
- L'Équipe de la Finance pour tous. (15 mars 2022). Qu'est-ce que SWIFT ? Consulté le 20 avil 2024 sur https://www.lafinancepourtous.com/outils/questions-reponses/quest-ce-que-swift/

- Contrast Security. (s.d.). What is penetration testing ? Consulté le 24 avril 2024 sur https://www.contrastsecurity.com/glossary/penetration-testing
- Ankush Das A. (2017). 21 Best Kali Linux Tools for Hacking and Penetration Testing. Consulté le 29 avril 2024 sur https://itsfoss.com/best-kali-linux-tools/

ANNEXES

ANNEXES 1 : organigramme de la BNA



Source : http://www.bna.tn/fr/particuliers/

ANNEXES 2 : 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.

ANNEXES 3 : un 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.

ANNEXES 4 : 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 MATIERES

Table des matières :