REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEURE ET DE LA RECHERCHE SCIENTIFIQUE

ECOLE SUPERIEURE DE COMMERCE

El Moudjahed – Mouloud Kacem Nait Belkacem
Pôle Universitaire - Koléa

Mémoire

Pour l'obtention du diplôme Post Graduation Spécialisée

Spécialité : Audit et Comptabilité

Thème :

Le rôle de l'Audit Interne dans le Risk Management (Cas : de la filiale Algérienne D)

Préparé par :

Mme BACHA Hadjira Epse DRIF

Encadré par :

Pr. BOUHADIDA Mohamed

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEURE ET DE LA RECHERCHE SCIENTIFIQUE

ECOLE SUPERIEURE DE COMMERCE

El Moudjahed – Mouloud Kacem Nait Belkacem
Pôle Universitaire - Koléa

Mémoire

Pour l'obtention du diplôme Post Graduation Spécialisée

Spécialité : Audit et Comptabilité

Thème :

Le rôle de l'Audit Interne dans le Risk Management (Cas : de la filiale Algérienne D)

Préparé par :

Mme BACHA Hadjira Epse DRIF

Encadré par :

Pr. BOUHADIDA Mohamed

Remerciement

Je tiens à exprimer ma reconnaissance envers Dieu Tout-Puissant pour nous avoir donné la force et la patience nécessaire pour mener à bien ce projet.

Au terme de ce parcours de post-Graduation, la rédaction de ce mémoire de fin d'études a été une expérience intense, exigeante et enrichissante. Je tiens à exprimer ma gratitude envers toutes les personnes qui ont contribué de près ou de loin à la réalisation de ce travail.

Je tiens tout d'abord à remercier mon directeur de mémoire, ***Pr Bouhadida Mohamed***, pour sa guidance précieuse, son expertise, et sa patience tout au long de ce processus. Votre soutien inébranlable et vos conseils avisés ont été la clé de la réussite de ce mémoire.

Je tiens également à remercier le corps enseignant de l'Ecole Supérieure de Commerce pour la qualité de l'enseignement dispensé. Leur cours, discussions et retours d'expérience ont grandement contribué à l'élaboration de ce mémoire.

Un grand merci à ma famille pour leur soutien indéfectible. Vos encouragements, votre compréhension et votre patience ont été essentiels dans cette expérience.

Mes amis et collègues méritent également ma reconnaissance pour leur soutien moral et leur encouragement tout au long de ce parcours.

Enfin, je tiens à remercier toutes les sources, auteurs, et chercheurs dont les travaux ont enrichi mon mémoire.

La rédaction de ce mémoire a été un défi stimulant, et je suis reconnaissante d'avoir eu l'opportunité de le mener. Ce travail représente bien plus que des pages imprimées ; il incarne les connaissances acquises, les compétences développées, et l'expérience accumulée au cours de mon parcours universitaire et professionnel.

Merci à tous ceux qui ont rendu cela possible. Ce mémoire est le fruit de notre collaboration, de nos échanges, et de nos efforts conjoints.

Avec gratitude,
Hadjira Bacha Epse DRIF

SOMMAIRE

Remerciement

Sommaire..... I

Liste des abréviations..... II-III

Liste des tableaux..... IV

Liste des figures..... V

Résumé..... VI

Introduction Générale..... A-F

Chapitre 01 : L'Audit Interne ses appuis et ses conditions de mise en œuvres. 1

Introduction du chapitre..... 2

Section 01 : Fondements de l'Audit Interne..... 3

Section 02 : Appuis à l'Audit Interne..... 16

Section 03 : Conditions de mise en œuvre de l'Audit Interne..... 22

Conclusion du chapitre..... 27

Chapitre 02 : Le Risk Management..... 28

Introduction du chapitre..... 29

Section 01 : Aperçu sur le Risk Management..... 30

Section 02 : La démarche du Risk Management..... 37

Section 03 : Intégration du Risk Management dans la gestion d'entreprise..... 53

Conclusion du chapitre..... 58

Chapitre 03 : Cas Pratique..... 59

Introduction du chapitre..... 60

Section 1 : Présentation de la Cible..... 61

Section 2 : Audit Interne du département de la sureté..... 68

Section 3 : Audit Externe..... 79

Conclusion du chapitre..... 86

Conclusion Générale..... 88

Bibliographie..... 93

Table des matières..... 96

LISTE DES ABREVIATIONS

RM	Risk Management
SMP	Security Management procedures
ERM	Entreprise Risk Management
ISO	The International Organization for Standardization
ISA	International Standards of Audit
Groupe « D »	Maison mère
Filiale Algérienne « D »	La cible ou l'entreprise concernée par l'étude de cas
EVP	Equivalent vingt pieds
COSO	Committee of Sponsoring Organizations
CCTV	Closed-Circuit TeleVision
GRE	Gestion des risques entreprise
AI	Audit Interne
CI	Contrôle Interne
KPIs	Keys Performance Indicators
BCP	Business Continuity Plan (Plan de Continuité des Activités)
DRP	Disaster Recovery Plan (Plan de Reprise d'Activité)
VaR	Value at Risk (Valeur en Risque)
CSO	Chief Security Officer (Responsable de la Sécurité)
IFACI	Institut français de l'Audit et du Contrôle Interne
IAASB	International Auditing and Assurance Standards Board
IIA	Institute of Internal Auditors
CFO	Chief Financial Officier (Directeur Financier)
CEO	Chief Executive Officer (Directeur Général)
RGPD	Règlement Général sur la Protection des Données
VPN	Virtual Private Network (réseau privé virtuel)
PMI	Project Management Institute
NIST	National Institute of Standards and Technology
JIT	Just In Time (Juste à temps)
PMBOK	Project Management Body of Knowledge

LISTE DES ABREVIATIONS

BPM	Business Process Management
BA	Banque d'Algérie
SCF	Système Comptable et Financier
IFRS	International financial reporting standards

LISTE DES TABLEAUX

Désignation	Page
Tableau n°01 : Démarche Générale de l'Audit Interne (Source : élaboré par nos soins)	**p.25**
Tableau n°02 : L'effectif de la « Filiale Algérienne D » (Source : Documents internes, 2023)	**p.66**
Tableau n°03 : Liste des intervenants. (Source : élaboré par nos soins)	**p.69**
Tableau n°04 : Le calendrier prévisionnel. (Source : élaboré par nos soins)	**p.71**
Tableau n°05 : La répartition des sections de travail. (Source : élaboré par nos soins)	**p.72**
Tableau n°06 : Le Registre des risques « Risque Register » et/ou les non-conformités identifiées. (Source : élaboré par nos soins)	**p.73**
Tableau N°07 : Classement des risques par ordre de priorité, du plus critique au moins critique. (Source : élaboré par nos soins)	**p.75**
Tableau N°08 : Les recommandations détaillées à mettre en place pour chaque risque. (Source : élaboré par nos soins)	**p.77**

LISTE DES FIGURES

Désignation	Page
Figure n°01 : Processus de Gestion des Risques (Source : Norme ISO 31000)	**p.39**
Figue n°02 : Analyse SWOT (Source :Analyse SWOT En Français (bing.com))	**p.41**
Figure n°03 : Table de Criticité (Source : Norme ISO 31000)	**p.43**
Figure n°04 : Stratégie du Risque (Source : Norme ISO 31000)	**p.45**
Figure N°05 : Roue de Deming, Source : La roue de Deming.pdf notice & manuel d'utilisation.	**p.46**
Figure N°06 : Le cycle d'amélioration, Source : La roue de Deming.pdf notice & manuel d'utilisation.	**p.52**
Figure N°07 : Incorporation de la gestion des risques dans la stratégique de l'entreprise , Source : Gestion des risque opérationnelle Images (bing.com)	**p.55**
Figure N°08 : L'organigramme de la « Filiale Algérienne D », Source : Document Interne, exercice 2023.	**p.65**
Figure n°09 : La cartographie des risques, Source : élaboré par nos soins.	**p.74**

La maitrise des risques ou « Gestion des risques » est devenue depuis quelques années au cœur des préoccupations des autorités, actionnaires et des dirigeants des différentes entreprises, et cela avec la multiplication des crises et scandales à travers le monde.

Il est inévitable qu'une entreprise prenne des risques, sinon elle ne saura plus créer de la valeur, mais elle est tenue tout de même de les maitriser afin de ne pas remettre en cause sa crédibilité et essentiellement sa pérennité.

Dans cette optique, nous nous sommes intéressés dans la présente étude, à l'un des outils les plus actuellement recommandés en la matière, à savoir l'Audit Interne. Après une étude détaillée qui nous a permis de répondre aux questions secondaires émises au début. En effet, la troisième hypothèse a été confirmée, et l'Audit Interne est un outil et un dispositif indispensable pour l'analyse des risques.

Mots clés : Audit Interne, Risk Management, Outil, Gestion des risques , non-conformité.

Summary :

"The mastery of risks, or 'Risk Management,' has become a central concern for authorities, shareholders, and leaders of various companies in recent years, especially with the proliferation of crises and scandals worldwide. It is inevitable for a company to take risks; otherwise, it would fail to create value. However, it is still obligated to control these risks to safeguard its credibility and, essentially, its sustainability.

In this context, we focused on one of the currently recommended tools in this field in the present study, namely Internal Audit. After a detailed study that allowed us to address the initial secondary questions, it was confirmed that the third hypothesis is valid. Internal Audit is indeed an indispensable tool and mechanism for risk analysis."

Key words : Internal Audit, Risk Management, Tool, Non-conformity.

INTRODUCTION GENERALE

Chaque entreprise justifie son existence à travers la poursuite de ses objectifs. Et c'est en fonction de ces objectifs qu'on peut mener des contrôles de différentes natures et différents niveaux., parmi lesquels figure le Risk Management.

Si dans le futur une entreprise souhaite améliorer ses performances opérationnelles ou autres, elle devra en effet s'assurer régulièrement qu'elle se rapproche petit à petit de ses objectifs. Le Risk Management représente l'un des moyens pour y arriver et l'Audit Interne un de ces outils.

L'audit Interne, occupe une place cruciale dans le paysage des entreprises contemporaines. La gestion des risques est devenue une préoccupation majeure pour les organisations, confrontées à un environnement commercial de plus en plus complexe et dynamique. Dans ce contexte, l'audit émerge comme un instrument essentiel permettant de mieux appréhender, évaluer et maîtriser les risques auxquels une entreprise peut être exposée.

En conséquence, le rôle de l'Audit Interne dans le Risk Management est de plus en plus important car les professionnels de l'audit Interne et de la gestion des risques sont confrontés à des évolutions et des changements dans l'environnement des affaires, la réglementation et l'avancée et/ou la complexité technologique.

Dans ce mémoire, nous examinerons le rôle de l'Audit Interne dans le Risk Management, en mettant l'accent sur son impact sur la performance globale des organisations et la résilience. Nous analyserons comment l'audit interne peut contribuer à la gestion des risques liés à la sureté, tout en engageant un processus de certification aux normes internationales – ISO 28000 –.

A travers cette étude, nous tenterons de répondre à la question principale suivante :

Comment restaurer le système de sureté actuel en un système performant capable de gérer efficacement les menaces et les incidents au sein de la chaîne d'approvisionnement de la sureté ?

Pour bien traiter cette problématique, nous avons jugé utile de la subdiviser en sous-questions :

- Qu'est-ce que l'Audit Interne ?
- Qu'est-ce que le Risk Management ?
- Existe-il une relation entre l'Audit Interne et le Risk Management ?
- Comment mesurer et évaluer en continu l'efficacité du système de gestion de la sureté ?
- Comment apporter des améliorations constantes dans le système en fonction des retours d'expérience de d'autres filiales du Groupe ?

Les hypothèses de recherche :

Hypothèse 1 : Les technologies de surveillance avancées, telles que la vidéosurveillance intelligente, contribuent à une détection plus rapide et plus précise des menaces dans la chaîne d'approvisionnement de la sûreté.

Hypothèse 2 : L'amélioration des programmes de formation du personnel sur la sensibilisation aux menaces et aux protocoles de sécurité conduit à une meilleure réactivité face aux incidents.

Hypothèse 3 : Les entreprises qui s'alignent rigoureusement sur les normes et réglementations de sûreté réussissent mieux à instaurer des systèmes performants de gestion des menaces et des incidents dans leur chaîne d'approvisionnement.

L'objectif de la recherche :

L'objectif principal de cette recherche est d'analyser comment l'Audit Interne peut contribuer de manière efficace à la gestion proactive des risques, en offrant des mécanismes permettant d'identifier, d'évaluer et de traiter les risques opérationnels, financiers, stratégiques et autres.

Ce mémoire vise à atteindre plusieurs objectifs pertinents que nous souhaitons aborder :

- Explorer en profondeur le domaine du Risk Management, en proposant une analyse approfondie du système de la sureté.
- Analyser comment l'Audit Interne permet de mettre à jour le contrôle interne.
- Montrer comment une entreprise peut soumettre en pratique l'un de ses processus à une certification aux normes internationales (Norme ISO 28000).
- Comprendre comment le Risk Management permet d'atteindre les objectifs de l'entreprise.
- Le rôle de l'audit interne et le Risk Management dans l'amélioration continue.

La méthodologie de recherche :

Dans ce mémoire de Post-Graduation Spécialisé, une approche basée sur une étude de Cas a été adoptée pour répondre à l'objectif de recherche.

Cette étude de cas se concentre sur l'entreprise « Filiale Algérienne D », afin d'analyser en détail l'Audit Interne et son rôle dans le Risk Management.

La collecte des données a été réalisée à partir de différentes sources, telles que :

- Des entretiens avec le personnel du département de sureté.
- Analyses des documents internes de l'entreprise (Politique de sureté, les procédures, rapport du Groupe sur la sureté, rapports des réunions « Management Meetings » etc…).

- Une revue approfondie de la littérature existante sur l'Audit Interne, le Risk Management : pour situer la recherche dans son contexte théorique et identifier les principaux concepts.

Ces données ont été analysées de manière qualitative, en utilisant des méthodes d'analyse de contenu pour extraire l'information pertinente.
De plus, afin de compléter l'analyse, nous avons effectué un Audit Interne cela permet d'obtenir des mesures et des résultats permettant d'appuyer notre étude de cas.

La posture épistémologique :

La posture épistémologique de cette recherche est basée sur une approche positiviste. Dans cette perspective, l'objectif est d'obtenir des connaissances objectives et véritables sur le rôle de l'Audit Interne dans le Risk Management. La recherche s'appuie sur des données réelles afin d'analyser les relations de cause à effet entre les deux concepts (Audit Interne et Risk Management).

Le choix et intérêt du sujet :

Au moment où s'achève mon parcours de post-graduation, la rédaction de ce mémoire marque une étape significative de ma formation. Ce travail, intitulé "Le rôle de l'Audit Interne dans le Risk Management", explore la relation complexe entre l'audit et la gestion des risques au sein des organisations.

Le choix de ce sujet découle d'une double passion :

- D'une part, mon intérêt pour les pratiques d'audit, leur évolution constante et leur rôle crucial dans la prise de décisions éclairées au sein des entreprises ;

- D'autre part, mon désir d'explorer comment l'audit peut être un outil efficace pour anticiper, identifier et atténuer les risques, élément essentiel dans le contexte économique actuel.

Le plan de rédaction :

La thèse se structure autour de plusieurs axes de réflexion.

Tout d'abord, le premier chapitre examine la nature même de l'Audit Interne « ses appuis et ses conditions de mise en place » en tant qu'instrument de contrôle et de vérification, en soulignant son adaptation aux exigences changeantes des entreprises et des marchés.

Ensuite, le deuxième chapitre se penche sur la notion de Risk Management, explorant les différentes étapes de l'approche illustrés dans la norme ISO 31000.

Et un dernier chapitre, qui présente une étude de cas concrète portant sur l'entreprise « Filiale Algérienne du Groupe D », dont nous utilisons un exemple réel pour donner une attention particulière à l'intégration de l'Audit Interne dans les processus de gestion des risques, en mettant en place de mécanismes de contrôle efficaces et recommandations de stratégies d'atténuation appropriées.

En conclusion, cette recherche vise à approfondir la compréhension de la manière dont l'Audit Interne peut être outil efficacement dans le processus de gestion des risques, contribuant ainsi à renforcer la résilience et la performance des organisations dans un monde des affaires en constante évolution.

Chapitre 01

L’Audit Interne : ses appuis et ses conditions de mise en œuvre

Introduction du chapitre :

L'audit interne constitue une fonction cruciale au sein des organisations, que ce soit dans le secteur public ou privé, offrant une perspective indépendante et objective sur la gestion des risques, le contrôle interne et la gouvernance.

Ce chapitre explore les fondements essentiels de l'audit interne, en se concentrant particulièrement sur ses appuis et les conditions nécessaires à sa mise en œuvre efficace. De la définition de son mandat à l'identification des ressources indispensables, en passant par la collaboration avec les parties prenantes et l'adaptation aux évolutions du contexte organisationnel, ce chapitre vise à fournir un aperçu approfondi des éléments clés qui façonnent le succès de l'audit interne. En examinant les piliers fondamentaux sur lesquels repose cette fonction, nous chercherons à dévoiler les mécanismes permettant de maximiser son impact et d'assurer une contribution significative à l'amélioration continue de la performance organisationnelle.

Section 01 :

Fondements de l'Audit Interne

1- Définition et Objectif de l'Audit Interne :

1.1- Définition de l'Audit Interne

L'audit interne peut être défini comme une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée. Cette définition provient du Cadre International pour la Pratique Professionnelle de l'Audit Interne émis par l'Institut des Auditeurs Internes (IIA - Institute of Internal Auditors). [1]

L'audit interne est une activité indépendante et objective qui aide l'organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle, et de gouvernance, et en faisant des propositions pour renforcer leur efficacité.[2]

Contrairement à l'audit externe, qui est généralement réalisé par des experts externes à l'organisation, l'audit interne est mené par des professionnels internes, les auditeurs internes.

La mise en place d'une organisation professionnelle au niveau international IAASB- et en particulier IFACI en France – ont joué et jouent encore un rôle de véritables incubateurs d'une théorie et d'une pratique qui donne à l'Audit Interne ses lettres de noblesse et en assurant l'universalité.

[1] "Institut des Auditeurs Internes (IIA) - Cadre International pour la Pratique Professionnelle de l'Audit Interne", disponible sur le site officiel de l'IIA : https://na.theiia.org/standardsguidance/Public%20Documents/IIA%20International%20Professional%20Practices%20Framework%20(French).pdf

[2] Cadre de référence internationale (IIA) – cadre de référence internationale des pratiques professionnelles -Edition 2017.

1.2- Objectif de l'Audit Interne

L'objectif de l'audit interne peut varier en fonction de la nature et des besoins spécifiques de chaque organisation. Cependant, on peut généralement définir quelques objectifs généraux de l'audit interne. Il est important de noter que ces objectifs peuvent être adaptés en fonction des normes professionnelles, des attentes de la direction et des caractéristiques propres à chaque organisation. Voici quelques objectifs généraux de l'audit interne :[3]

1.2.1- Évaluation du contrôle interne :

« Le contrôle interne désigne l'ensemble des politiques, des procédures et des mécanismes mis en place par une organisation pour assurer la réalisation de ses objectifs opérationnels, financiers et de conformité. Cela englobe la gouvernance d'entreprise, la gestion des risques et le contrôle des activités. » [4]

L'évaluation du contrôle interne est la vérification de l'efficacité des systèmes de contrôle interne de l'organisation pour assurer la protection des actifs, la fiabilité des informations financières et le respect des lois et des réglementations.

Les composants du contrôle interne :

- ✓ *Contrôle opérationnel :* Ensemble des procédures visant à garantir l'efficacité et l'efficience des opérations de l'entreprise.

- ✓ *Contrôle financier :* Processus assurant la fiabilité des informations financières et la conformité aux normes comptables.

- ✓ *Contrôle de conformité :* Garantie du respect des lois et régulations auxquelles l'organisation est soumise.

[3] Pratique de l'Audit. « Editions BERTI », Auteur : Mokhtar BELAIBOUD, docteur d'Etat en sciences de gestion, Expert-comptable et commissaire aux comptes.

[4] "Contrôle Interne - Des fondamentaux aux bonnes pratiques" par Anne Germain et Jean-Pierre Hugot.

1.2.2- Gestion des risques :

L'objectif principal de l'audit interne est d'apporter une assurance et une valeur ajoutée à une organisation en évaluant et en améliorant l'efficacité de ses processus de gouvernance, de gestion des risques et de contrôle interne. La gestion des risques est un aspect clé dans ce mémoire, et l'audit interne joue un rôle crucial dans ce domaine. Voici comment l'objectif de l'audit interne est lié à la gestion des risques :[5]

a- Identification des Risques :

L'audit interne contribue à identifier les risques auxquels une organisation est exposée. Cela implique d'analyser les processus, les activités et les opérations pour repérer les éléments susceptibles de compromettre les objectifs de l'organisation.

b- Évaluation des Risques :

Une fois les risques identifiés, l'audit interne évalue leur impact potentiel sur les activités de l'organisation. Cette évaluation comprend souvent une analyse quantitative et qualitative pour déterminer la probabilité et la gravité des risques.

c- Surveillance des Contrôles Internes :

L'audit interne examine les contrôles internes mis en place pour atténuer les risques. Il évalue l'efficacité de ces contrôles en s'assurant qu'ils sont adéquats et fonctionnent comme prévu pour réduire les risques à des niveaux acceptables.

d- Recommandations d'Amélioration :

Sur la base de ses évaluations, l'audit interne formule des recommandations pour renforcer les processus de gestion des risques. Ces recommandations visent à améliorer l'efficacité des contrôles internes et à réduire les vulnérabilités aux risques identifiés.

e- Assurance à la Direction et aux Parties Prenantes :

En fournissant des opinions objectives et des assurances sur l'efficacité des processus de gestion des risques, l'audit interne offre à la direction et aux parties prenantes une confiance dans la capacité de l'organisation à atteindre ses objectifs tout en minimisant les risques.

[5] Théorie et pratique de l'Audit Interne, Jacques Renard éditions EYROLLES

f- Adaptation aux Changements :

L'environnement des affaires est en constante évolution. L'audit interne s'adapte en continu pour évaluer l'impact des changements internes et externes sur les risques, aidant ainsi l'organisation à ajuster sa stratégie de gestion des risques.

1.2.3- Conformité aux politiques et procédures :

S'assurer que les activités de l'organisation sont conformes aux politiques, procédures, lois et réglementations applicables. Voici quelques étapes générales et sommaire d'audit interne pour assurer la conformité aux politiques et procédures :

a- Identification des politiques et procédures :

Consiste à identifier toutes les politiques et procédures pertinentes pour votre organisation. Cela peut inclure des politiques internes, des réglementations gouvernementales, des normes de l'industrie, etc.

b- Communication et sensibilisation :

S'assurer que toutes les parties prenantes de l'organisation, y compris les employés, sont informées des politiques et procédures en place. Organisez des sessions de formation si nécessaire.

c- Création de manuels et guides :

Élaborer des manuels et guides détaillés qui expliquent les politiques et procédures de manière claire et accessible. Ces documents peuvent servir de référence pour les employés et les gestionnaires.

d- Responsabilité et rôles définis :

Attribuer des responsabilités spécifiques aux personnes chargées de mettre en œuvre et de surveiller la conformité aux politiques et procédures. Clarifiez les rôles et les attentes.

e- Systèmes de surveillance et d'évaluation :

Il s'agit de la mise en place des systèmes de surveillance régulière pour évaluer la conformité. Cela peut inclure des audits internes, des examens de conformité et des rapports réguliers.

f- Révision régulière des politiques :

Les politiques et procédures doivent être régulièrement révisées pour s'assurer qu'elles restent à jour par rapport aux changements internes et externes. Impliquez les parties prenantes dans ce processus.

g- Formation continue :

Organiser des sessions de formation continue pour les employés afin de les tenir informés des mises à jour des politiques et procédures. Assurez-vous qu'ils comprennent les implications de la non-conformité.

h- Communication ouverte et canaux de signalement :

Encourager une communication ouverte au sein de l'organisation. Mettez en place des canaux de signalement pour que les employés puissent signaler tout problème de conformité sans crainte de représailles.

i- Réponse aux non-conformités :

Développer des procédures pour répondre aux cas de non-conformité. Cela peut inclure des actions correctives, des sanctions disciplinaires, des ajustements de politique, etc.

j- Documentation :

Garder des documents détaillés sur les processus de conformité, les formations, les évaluations, les révisions de politique, etc. Cela facilite les audits internes et externes.

1.2.4- Amélioration des processus opérationnels :

L'amélioration des processus opérationnels est une démarche essentielle pour accroître l'efficacité, la productivité et la qualité d'une organisation. Voici quelques étapes générales pour améliorer les processus opérationnels :

a- Identification des processus existants :

Cartographier et documenter tous les processus opérationnels existants dans votre organisation. Identifier les parties prenantes et comprenez leurs attentes et besoins.

b- Analyse des processus actuels :

Évaluer la performance des processus actuels en termes de délais, coûts, qualité et satisfaction client. Identifier les points faibles, les goulets d'étranglement et les opportunités d'amélioration. [6]

c- Établissement d'objectifs clairs :

Définir des objectifs spécifiques, mesurables, atteignables, pertinents et temporels (SMART) pour chaque processus à améliorer.

d- Impliquer les parties prenantes :

Impliquer toutes les parties prenantes concernées par le processus, y compris les employés, les clients et les fournisseurs. Recueillir leurs opinions et suggestions pour obtenir une vision complète.

e- Reconception des processus :

Identifier les étapes inutiles ou redondantes et éliminez-les. Simplifier les flux de travail en automatisant les tâches répétitives lorsque c'est possible. Réorganiser les processus pour les rendre plus efficaces.

f- Intégration de la technologie :

Explorer les technologies qui peuvent améliorer les processus, comme les logiciels de gestion, les outils de collaboration, ou l'automatisation des processus métier (BPM).[7]

g- Formation et communication :

S'assurer que les employés comprennent les nouvelles procédures et ont les compétences nécessaires pour les mettre en œuvre. Communiquer de manière transparente sur les changements à venir et les avantages attendus.

[6] "Business Process Reengineering: Breakpoint Strategies for Market Dominance" par Michael Hammer et James A. Champy.

[7] "The Phoenix Project: A Novel About IT, DevOps, and Helping Your Business Win" par Gene Kim, Kevin Behr, et George Spafford.

h- Mise en œuvre progressive :

Mettre en œuvre les changements progressivement pour minimiser les interruptions.

Effectuer des tests pilotes pour identifier et résoudre les problèmes potentiels.

i- Mesure de la performance :

Établir des indicateurs clés de performance (KPI) pour mesurer la réussite des changements.

Surveiller régulièrement les performances et ajustez les processus si nécessaire.

j- Boucle de rétroaction continue :

Encourager la rétroaction continue de la part des employés et des parties prenantes.

Réévaluer périodiquement les processus pour identifier de nouvelles opportunités d'amélioration.

1.2.5- Gouvernance d'entreprise :

L'évaluation de la structure de gouvernance vise à assurer que les activités de l'entreprise sont transparentes et que les parties prenantes ont accès à des informations pertinentes.

L'évaluation du conseil d'administration a pour objectif d'optimiser la performance de cet organe en s'assurant qu'il prend des décisions éclairées et alignées sur les objectifs de l'entreprise.

1.2.6- Communication des résultats :

La communication des résultats d'audits de manière transparente et constructive est essentielle pour garantir la confiance des parties prenantes et faciliter l'amélioration continue des processus et des systèmes.

2- Normes et cadre réglementaire :

Les normes et le cadre réglementaire de l'audit interne varient d'un pays à l'autre, mais il existe des normes internationales largement reconnues qui fournissent des lignes directrices pour la pratique de l'audit interne. Ces normes sont émises par l'Institute of Internal Auditors (IIA), une organisation internationale professionnelle dédiée à la promotion de l'audit interne.

2.1- Normes internationales pour la pratique professionnelle de l'audit interne (IIA) :

Les normes internationales pour la pratique professionnelle de l'audit interne sont souvent désignées sous le nom de "Normes internationales pour l'exercice professionnel de l'audit interne" (International Standards for the Professional Practice of Internal Auditing - IPPF). Les principales normes comprennent :

- Définition de l'audit interne
- Code de déontologie
- Normes de qualification
- Normes de gestion de la qualité
- Normes de mise en œuvre

2.2- Lois et réglementations locales :

En plus des normes internationales de l'IIA, les praticiens de l'audit interne doivent se conformer aux lois et réglementation locales spécifiques à leur juridiction. Ces lois peuvent prendre la forme du code de commerce, code civile, code des marchés publiques, code de l'investissement, code fiscale, code douanier, etc.

2.3- Normes comptables :

Les auditeurs internes sont souvent tenus de respecter les normes comptables en vigueur dans leur pays. Ces normes régissent la manière dont les transactions financières doivent être enregistrées, présentées et divulguées dans les états financiers.

En Algérie, les normes comptables sont édictées par le Conseil National de la Comptabilité (CNC), qui est l'organisme chargé de l'élaboration et de la mise à jour des normes comptables. Le CNC veille à l'harmonisation des pratiques comptables et à l'amélioration de la qualité de l'information financière.

Le référentiel Algérien, SCF est un ensemble de normes comptables principalement basées sur les normes internationales d'information financière (IFRS) pour le secteur privé et sur les normes comptables publiques pour le secteur public.

2.4- Normes sectorielles :

Certains secteurs d'activité peuvent avoir des normes spécifiques auxquelles l'audit interne doit se conformer. Par exemple, les institutions financières peuvent être régies par des réglementations spécifiques au secteur financier, exemple : règlements de la Banque d'Algérie (BA).

2.5- Normes de gouvernance d'entreprise :

Les praticiens de l'audit interne doivent également tenir compte des normes de gouvernance d'entreprise qui guident la manière dont les organisations sont dirigées et contrôlées.

3- Rôle et positionnement de l'Audit Interne dans l'organisation :

3.1- Rôle stratégique de l'Audit Interne :

L'audit interne joue un rôle important au sein d'une organisation en fournissant une assurance objective et indépendante sur la gestion des risques, le contrôle interne et les processus opérationnels.

Voici quelques-uns des principaux rôles de l'audit interne dans une organisation :

3.1.1- Contrôle Interne : L'audit interne examine l'efficacité des contrôles internes mis en place par l'organisation pour assurer la fiabilité des informations financières, la conformité aux lois et réglementations, et la protection des actifs.

3.1.2- Conformité : Il s'assure que l'organisation respecte les lois et les réglementations en vigueur. Cela peut inclure des domaines tels que la conformité fiscale, les normes comptables, les lois du travail, etc.[8]

[8] Audit et Contrôle Interne « Benoit pigé », éditions EMS « Management et société »

3.1.3- Efficacité Opérationnelle : L'audit interne évalue l'efficacité des processus opérationnels et propose des améliorations pour accroître l'efficacité, la productivité et la rentabilité.

3.1.4- Gestion des Actifs : Il examine la gestion des actifs de l'organisation, s'assurant qu'ils sont utilisés efficacement et protégés contre les pertes et les abus.

3.1.5- Gestion des Projets : L'audit interne peut également jouer un rôle dans l'évaluation des projets pour s'assurer qu'ils sont gérés de manière efficace, respectent les échéances et sont conformes aux objectifs stratégiques de l'organisation.

3.1.6- Prévention et Détection de la Fraude : En examinant les processus et les transactions, l'audit interne peut contribuer à la prévention et à la détection de la fraude au sein de l'organisation.

3.1.7- Amélioration Continue : L'audit interne participe à la culture d'amélioration continue en identifiant les opportunités d'amélioration et en suivant la mise en œuvre des recommandations.

3.2- Positionnement de l'Audit Interne dans l'organisation :

L'audit interne occupe une position cruciale au sein d'une organisation et joue un rôle essentiel dans la gouvernance, le contrôle et la gestion des risques. Voici quelques aspects clés du positionnement de l'audit interne dans une organisation :

3.2.1- Indépendance et Objectivité :

L'audit interne doit être indépendant et objectif. Il est généralement rattaché directement au conseil d'administration ou à un comité d'audit pour assurer son indépendance par rapport aux opérations quotidiennes de l'entreprise.

3.2.2- Relation avec le Conseil d'Administration :

L'audit interne maintient une relation étroite avec le conseil d'administration ou un comité d'audit. Cela garantit une communication directe sur les résultats de l'audit et les préoccupations liées aux risques et aux contrôles internes.

3.2.3-Hiérarchie Organisationnelle :

L'audit interne peut être dirigé par un directeur de l'audit interne, qui peut avoir le titre de Chief Audit Executive (CAE). Le CAE peut être membre du comité de direction de l'entreprise, ce qui démontre l'importance stratégique de la fonction d'audit interne.

3.2.4-Accès à l'Ensemble de l'Organisation :

L'audit interne a généralement accès à tous les secteurs de l'entreprise. Cela lui permet d'évaluer les activités, les processus et les systèmes à travers l'organisation afin de s'assurer que les objectifs sont atteints et que les risques sont maîtrisés.

3.2.5-Coordination avec les Autres Fonctions de Contrôle :

L'audit interne travaille en étroite collaboration avec d'autres fonctions de contrôle interne, telles que la conformité, la gestion des risques, et parfois avec les auditeurs externes. Cette coordination garantit une approche globale et cohérente de la gouvernance d'entreprise.

3.2.6-Rapports Réguliers :

L'audit interne fournit régulièrement des rapports au conseil d'administration ou au comité d'audit. Ces rapports peuvent inclure des évaluations des risques, des constatations d'audit, des recommandations d'amélioration et des mises à jour sur les activités d'audit en cours.

3.2.7- Évaluation de la Performance :

L'efficacité de la fonction d'audit interne est évaluée périodiquement. Cela peut être réalisé par le conseil d'administration, le comité d'audit ou par des évaluateurs externes pour s'assurer que l'audit interne fonctionne de manière efficace et efficiente.

Donc pour résumer les fondements de l'Audit Interne reposent sur plusieurs principes clés :[9]

A- Indépendance et Objectivité :

L'audit interne doit être indépendant et objectif. Cela signifie que les auditeurs internes doivent être libres de toute influence qui pourrait compromettre leur jugement impartial. Ils doivent également être objectifs dans la collecte et l'évaluation des preuves.

B- Conformité :

L'audit interne doit évaluer le respect des politiques, procédures, lois et réglementations en vigueur. Cela inclut l'examen de la conformité aux normes internes et externes qui s'appliquent à l'organisation.

C- Réalisation des Objectifs :

L'audit interne évalue la manière dont les objectifs de l'organisation sont atteints. Cela peut inclure l'évaluation des processus opérationnels, financiers, de conformité et de gestion des risques.

D- Risques et Contrôles :

Les auditeurs internes doivent évaluer les risques auxquels l'organisation est exposée et examiner l'efficacité des contrôles mis en place pour atténuer ces risques. Ils contribuent ainsi à renforcer le système de gestion des risques.

[9] Principles of Auditing: An International Perspective par Rick Stephan Hayes, Arnold Schilder, Roger Dassen, Philip Wallage McGraw-Hill, 1999

E- Valeur Ajoutée :

L'audit interne ne se limite pas à la simple identification des erreurs ou des faiblesses. Il vise également à fournir des conseils constructifs et des recommandations pour améliorer les processus, renforcer les contrôles internes et accroître la valeur ajoutée pour l'organisation.

F- Méthodologie Professionnelle :

Les auditeurs internes doivent suivre des normes et des méthodologies professionnelles lors de l'exécution de leurs missions. Ces normes peuvent varier en fonction du cadre réglementaire et des normes professionnelles applicables à l'audit interne.

G- Communication et Rapports :

Les résultats des missions d'audit interne doivent être communiqués de manière claire et efficace aux parties prenantes concernées. Les rapports d'audit doivent contenir des conclusions, des recommandations et des plans d'action appropriés.

H- Formation Continue :

Les auditeurs internes doivent maintenir et développer leurs compétences tout au long de leur carrière pour rester efficaces dans un environnement en évolution constante.

Section 02 :

Appuis à l'Audit Interne

1- Soutien de la Direction et Engagement de la haute Direction :

L'engagement de la haute direction est essentiel pour assurer l'efficacité de l'audit interne au sein d'une organisation. Voici quelques raisons pour lesquelles l'implication de la direction est cruciale, ainsi que des moyens par lesquels la direction peut faciliter le travail de l'audit interne :

1.1- Soutien financier et ressources :

L'audit interne nécessite des ressources adéquates, tant en termes de personnel que de budget. L'engagement de la haute direction garantit que l'audit interne dispose des ressources nécessaires pour mener à bien ses missions.

1.2- Crédibilité :

L'engagement de la haute direction renforce la crédibilité de l'audit interne. Les auditeurs internes ont besoin de l'approbation et du soutien de la direction pour obtenir l'accès nécessaire aux informations et assurer que leurs recommandations sont prises au sérieux.

1.3- Priorité stratégique :

Lorsque l'audit interne est soutenu par la haute direction, il est plus susceptible d'être intégré dans la stratégie globale de l'organisation. Cela garantit que l'audit interne est aligné sur les objectifs et les priorités stratégiques de l'entreprise.[10]

[10] Audit Interne, Elisabeth Bertin, éditions EYROLLES.

1.4- Culture d'intégrité et de responsabilité :

L'engagement de la haute direction en faveur de l'audit interne contribue à promouvoir une culture d'intégrité et de responsabilité au sein de l'organisation. Cela envoie un message clair sur l'importance de la gouvernance et du respect des normes éthiques.

Voici aussi comment la direction peut faciliter le travail de l'audit interne :

1.5- Accès aux informations :

La direction doit faciliter l'accès de l'audit interne à toutes les informations nécessaires pour mener ses missions. Cela inclut l'accès aux documents financiers, opérationnels et stratégiques.

1.6- Collaboration :

La collaboration entre la direction et l'audit interne est essentielle. La direction doit encourager une communication ouverte et constructive afin que les auditeurs internes puissent comprendre les enjeux et les objectifs de l'entreprise.

1.7- Réponse aux recommandations :

La direction devrait répondre de manière proactive aux recommandations de l'audit interne. Cela démontre un engagement envers l'amélioration continue et renforce la confiance dans le processus d'audit.

1.8- Formation continue :

La direction peut faciliter le travail de l'audit interne en fournissant une formation continue aux membres de l'équipe interne sur les changements réglementaires, les risques émergents et les meilleures pratiques de l'industrie.

1.9- Mise en œuvre des recommandations :

La direction doit s'engager à mettre en œuvre les recommandations de l'audit interne. Cela garantit que les constatations de l'audit ne restent pas simplement des rapports, mais qu'elles se traduisent également par des actions concrètes.

2- Ressources Humaines et Compétences

Il est important de noter que les compétences nécessaires peuvent varier en fonction de l'industrie, de la taille de l'organisation et du contexte spécifique.

L'équipe d'audit interne doit posséder un ensemble de compétences variées pour mener à bien ses missions. Ces compétences peuvent être regroupées en plusieurs catégories, notamment :[11]

2.1- Compétences techniques :

- Connaissance approfondie des normes comptables et des principes de gouvernance.
- Compréhension des risques financiers et opérationnels.
- Maîtrise des techniques d'audit et de revue de processus implique :
- L'examen de documents tels que les politiques, les procédures, les contrats, les factures, les relevés bancaires,
- Les entretiens avec le personnel clé, les gestionnaires, les employés et d'autres parties prenantes permettent aux auditeurs de recueillir des informations qualitatives sur les processus, les contrôles internes, les risques et les pratiques en place,
- Les auditeurs peuvent observer directement les activités sur le terrain pour évaluer la conformité aux procédures établies et identifier d'éventuelles lacunes dans les processus.
- Les auditeurs évaluent les risques auxquels l'organisation est confrontée et concentrent leurs efforts d'audit sur les domaines présentant le plus grand risque.

2.2- Compétences en communication :

- Excellentes compétences en communication écrite et orale.
- Capacité à présenter des rapports d'audit de manière claire et concise.
- Aptitude à interagir avec différentes parties prenantes.

[11] Institute of Internal Auditors (IIA). (2021). "International Standards for the Professional Practice of Internal Auditing." [En ligne]. Disponible sur : https://na.theiia.org/standards-guidance/Public%20Documents/Standards/IIA-International-Standards-2021.pdf

2.3- Compétences en analyse et résolution de problèmes :

- Capacité à analyser des données complexes.
- Aptitude à identifier les problèmes et à proposer des solutions.
- Esprit critique et logique.

2.4- Compétences en gestion de projet :

- Capacité à planifier et à organiser des audits.
- Gestion efficace du temps pour respecter les échéances.
- Collaboration avec d'autres membres de l'équipe et parties prenantes.

2.5- Compétences en technologie de l'information :

- Compréhension des systèmes d'information et des technologies associées.
- Utilisation d'outils d'analyse de données et de logiciels d'audit.

2.6- Compétences en éthique et intégrité :

- Respect des normes éthiques et professionnels de l'audit interne.
- Intégrité et objectivité dans l'exécution des missions.

2.7- Compétences relationnelles :

- Capacité à établir des relations de confiance avec les collaborateurs.
- Collaboration efficace avec les différentes équipes au sein de l'organisation.

3- Technologie et outils d'audit

En intégrant des technologies, les cabinets d'audit peuvent améliorer leur efficacité opérationnelle, réduire les risques d'erreurs humaines et renforcer la qualité globale de leurs services d'audit.

Voici une présentation des principales technologies et outils utilisés dans le processus d'audit interne :

3.1- Logiciels d'audit automatisé :

Les outils d'audit automatisé permettent aux auditeurs internes de réaliser des tests de manière plus rapide et plus efficace. Ces outils peuvent automatiser la collecte de données, l'analyse des risques, les tests de conformité, et générer des rapports.

3.2- Systèmes de gestion des audits :

Les systèmes de gestion des audits aident à planifier, organiser et suivre l'avancement des audits. Ils peuvent également faciliter la collaboration entre les membres de l'équipe d'audit et permettre le stockage sécurisé des documents liés aux audits.

3.3- Analyse de données assistée par ordinateur (ADAO) :

Les outils d'ADAO aident les auditeurs à analyser de grandes quantités de données pour identifier des tendances, des anomalies et des risques. Ces outils peuvent accélérer l'analyse des données financières, opérationnelles et de conformité.

3.4- Technologies de collecte de données :

L'utilisation de technologies de collecte de données, telles que l'exploration de données, permet aux auditeurs de récupérer des informations à partir de différentes sources, y compris des bases de données, des fichiers électroniques et des systèmes informatiques.

3.5- Outils de gestion des risques :

Les outils de gestion des risques aident les auditeurs à évaluer les risques associés aux processus, activités et systèmes de l'entreprise. Ils facilitent également la documentation des contrôles internes mis en place pour atténuer ces risques.

3.6- Logiciels de suivi des recommandations :

Une fois l'audit effectué, les auditeurs utilisent des logiciels de suivi des recommandations pour suivre la mise en œuvre des actions correctives recommandées. Cela permet de s'assurer que les problèmes identifiés sont résolus de manière appropriée.

3.7- Outils de communication et de présentation :

Les auditeurs utilisent des outils de communication pour présenter leurs conclusions de manière claire et concise. Des logiciels de création de rapports et de visualisation des données peuvent être employés pour rendre l'information plus compréhensible pour les parties prenantes.

3.8- Formation en ligne et modules d'apprentissage :

Les auditeurs internes peuvent utiliser des plateformes de formation en ligne pour rester informés sur les dernières normes, réglementations et techniques d'audit. Cela garantit que l'équipe d'audit reste compétente et à jour.

Section 03 :

Conditions de mise en œuvre de l'Audit Interne

1- Planification et Programmation des Audits :

Le processus de planification des audits est une étape essentielle dans la réalisation d'audits internes ou externes. Il vise à définir clairement les objectifs de l'audit, à identifier les domaines à auditer, à élaborer un plan d'audit détaillé et à allouer les ressources nécessaires. Voici les étapes générales du processus de planification des audits, y compris la définition des objectifs et la sélection des domaines à auditer :[12]

1.1- Établissement des objectifs de l'audit :

- Définir clairement les objectifs et les attentes de l'audit. Les objectifs doivent être spécifiques, mesurables, réalisables, pertinents et limités dans le temps (SMART).
- Identifier les critères d'audit, qui serviront de référence pour évaluer la conformité et la performance.

1.2- Identification des domaines à auditer :

- Identifier les domaines ou les processus qui seront inclus dans l'audit en fonction des objectifs définis.
- Consulter les parties prenantes, tels que les responsables des départements concernés, pour obtenir des informations sur les risques et les préoccupations spécifiques.

1.3- Analyse des risques :

- Évaluer les risques associés à chaque domaine à auditer. Cette analyse peut se baser sur des facteurs tels que la complexité, la criticité, les antécédents d'audits précédents, les changements récents, etc.
- Prioriser les domaines en fonction de leur niveau de risque.

[12] « Théorie et pratique de l'Audit Interne », Jacques Renard,9éme édition EYROLLES.

1.4- Définition du plan d'audit :

- Élaborer un plan d'audit détaillé qui spécifie les activités, les ressources, les échéances et les méthodologies à suivre.
- Déterminer les critères d'évaluation et les méthodes d'audit à utiliser (entretiens, examen de documents, observations, etc.).

1.5- Allocation des ressources :

- Identifier les ressources nécessaires à la réalisation de l'audit, y compris les compétences requises, le personnel, le budget, etc.
- Assigner des responsabilités claires aux membres de l'équipe d'audit.

1.6- Communication et engagement des parties prenantes :

- Informer les parties prenantes, y compris la direction et les employés concernés, des objectifs et de la portée de l'audit.
- Obtenir leur coopération et leur soutien tout au long du processus d'audit.

1.7- Élaboration d'un programme d'audit :

- Établir un calendrier détaillé des activités d'audit, y compris les dates de début et de fin, les réunions préliminaires, les entretiens, etc. Le calendrier doit être basé sur les priorités définies et tenir compte des contraintes de ressources et des délais s'assurer que le calendrier est réaliste et réalisable.

1.8- Révision et approbation :

- Soumettre le plan d'audit à la direction et aux parties prenantes pour révision et approbation.
- Intégrer les commentaires et les ajustements nécessaires.

En suivant ces étapes et/ou l'approche d'Audit Interne, les planificateurs d'audit peuvent s'assurer que l'audit est bien structuré, axé sur les objectifs, et qu'il utilise efficacement les ressources disponibles.

2- Communication et rapports d'Audit Interne :

La communication efficace avec les parties prenantes et la structuration des rapports d'audit ainsi que la diffusion des résultats revêtent une importance cruciale dans le domaine de l'audit et de la gestion d'entreprise. Voici quelques points clés pour chacun de ces aspects :

2.1- Importance de la communication efficace avec les parties prenantes :

2.1.1- Transparence :

La communication transparente renforce la confiance des parties prenantes, qu'elles soient internes (direction, employés) ou externes (actionnaires, clients, autorités réglementaires).

2.1.2- Prise de décision éclairée :

Des communications claires aident les parties prenantes à prendre des décisions éclairées en comprenant les résultats de l'audit et les recommandations qui en découlent.

2.1.3- Gestion des attentes :

Une communication proactive permet de gérer les attentes des parties prenantes, évitant ainsi les malentendus et les interprétations incorrectes.

2.1.4- Alignement avec les objectifs stratégiques :

Une communication efficace assure que les résultats de l'audit sont alignés sur les objectifs stratégiques de l'entreprise, renforçant ainsi la pertinence des recommandations.

2.1.5- Réactivité aux préoccupations :

Une communication ouverte facilite la prise en compte des préoccupations des parties prenantes et permet une réponse rapide aux questions ou inquiétudes.

Donc, pour résumer ci-dessous la démarche générale de l'Audit Interne :

	Quoi	Qui	Où, quand, comment	Enregistrement
01	Elaboration du planning des audits	Responsable de la Qualité	En début d'année, sur serveur consultable par l'ensemble du personnel	Planning annuel des audits internes
02	Notification	Auditeurs internes ou externes	3 mois avant l'échéance, par Email	Email, tableaux des auditeurs qualifiés
03	Préparation de l'audit	Auditeurs internes ou externes	Définition du champ et de l'objet Etude des documents Détermination de la date et du lieu de l'audit	Programme Rapport d'audit
04	Notification	Audités ou services concernés	Par Email, 15 jours avant	Note de service
05	Réalisation de l'audit	Auditeurs internes ou externes	Réunion d'ouverture, objet de l'audit, réunion de clôture	Rapport d'audit Fiches d'écarts
06	Diffusion du Rapport	Auditeurs internes ou externes Responsable de la Qualité	Rédaction, validation et diffusion du rapport d'audit Dans les 15 jours suivant l'audit	Rapport d'audit Fiches d'écarts
07	Traitement des écarts	Responsable de la Qualité Pilote de processus/ chef de service	Sur les fiches d'écarts Plans d'actions correctives Sur serveur	Fiches d'écarts clôturées Suivi actions curatives ou correctives relatives aux écarts
08	Mesure de l'efficacité des plans d'actions	Responsable de la Qualité Auditeurs internes ou externes	Audit annuel, revue de direction, audit de poste	Réclamations clients Non-conformités internes Indicateurs spécifiques

Tableau 01 : Démarche Générale d'Audit Interne (Source : réalisé par nos soins)

2.2- Structuration des rapports d'audit et diffusion des résultats :

2.2.1- Clarté et concision :

Les rapports d'audit doivent être structurés de manière claire et concise pour faciliter la compréhension des parties prenantes et la mise en œuvre des recommandations.

2.2.2- Identification des risques et opportunités :

Les rapports doivent mettre en évidence les risques identifiés ainsi que les opportunités d'amélioration, offrant ainsi une vision complète de la situation.

2.2.3- Recommandations pratiques :

Les recommandations doivent être formulées de manière pratique et réalisable, permettant une mise en œuvre efficace par l'entreprise.

3- Suivi et amélioration continue :

3.1- Clarté et Compréhension :

Les rapports d'audit doivent être structurés de manière claire et pour faciliter la compréhension des parties prenantes.

3.2- Identification des risques et opportunités :

Les rapports doivent mettre en évidence les risques identifiés ainsi que les opportunités d'amélioration, offrant ainsi une vision complète de la situation.

3.3- Recommandations pratiques :

Les recommandations doivent être formulées de manière pratique et réalisable, permettant une mise en œuvre efficace par l'entreprise.

3.4- Suivi post-audit :

Un mécanisme de suivi post-audit, inclus dans le rapport, renforce l'engagement envers l'amélioration continue et permet de mesurer les progrès réalisés.[13]

3.5- Diffusion sélective :

La diffusion des résultats doit être effectuée de manière sélective, en tenant compte de la confidentialité des informations sensibles, tout en assurant une communication transparente et complète.

[13] « Théorie et pratique de l'Audit Interne », Jacques Renard,9éme édition EYROLLES.

Conclusion du chapitre :

En conclusion, ce premier chapitre a exploré en détail le rôle essentiel de l'audit interne au sein des organisations, mettant en lumière ses appuis et les conditions nécessaires à une mise en œuvre efficace. Nous avons souligné l'importance de l'audit interne en tant que mécanisme de gouvernance interne, contribuant à la création de valeur et à l'atteinte des objectifs organisationnels.

Les appuis à l'audit interne, qu'ils soient managériaux, financiers, ou technologiques, sont cruciaux pour garantir son indépendance, sa pertinence et son efficacité. Les ressources allouées, la formation continue du personnel, ainsi que le soutien de la haute direction, sont autant de piliers qui renforcent la capacité de l'audit interne à jouer un rôle proactif dans la gestion des risques et l'amélioration des processus internes.

Par ailleurs, les conditions de mise en œuvre ont été examinées sous l'angle des normes professionnelles, de l'éthique, et de la communication. L'alignement de l'audit interne sur les normes et les meilleures pratiques garantit la crédibilité de ses travaux et renforce la confiance des parties prenantes. L'éthique professionnelle demeure un principe fondamental, assurant l'intégrité des processus d'audit et la confidentialité des informations sensibles.

En fin de compte, la réussite de l'audit interne dépend de l'engagement de tous les acteurs au sein de l'organisation. Les synergies entre les différentes fonctions, la collaboration étroite avec les parties prenantes et la capacité à s'adapter aux évolutions du contexte organisationnel sont autant d'éléments clés qui positionnent l'audit interne comme un outil stratégique au service de la performance et de la pérennité de l'entreprise. En consolidant ces appuis et en respectant ces conditions, l'audit interne devient un levier puissant pour promouvoir une gouvernance robuste et orientée vers l'excellence.

Chapitre 02 :
Le Risk Management

Introduction du chapitre :

Le monde des affaires évolue constamment, exposant les organisations à un large éventail de risques, qu'ils soient financiers, opérationnels, stratégiques, environnementaux, ou liés à la conformité réglementaire. Les risques peuvent provenir de sources internes ou externes, et leur impact peut être plus ou moins sévère.

La gestion des risques ne vise pas à éliminer tous les risques, car cela serait impossible et paralyserait l'organisation. Au contraire, elle vise à les identifier, à les évaluer, et à prendre des mesures pour les atténuer ou les gérer de manière appropriée. En d'autres termes, il s'agit d'optimiser la balance entre le risque et la récompense.

Dans ce chapitre, nous explorerons plus en détail les concepts clés du Risk Management, y compris l'identification des risques, l'évaluation, la planification de la gestion des risques, la mise en œuvre de mesures, la surveillance et le suivi, ainsi que la révision et l'adaptation continue. Nous examinerons également les différentes méthodologies, les outils et les meilleures pratiques utilisés dans la gestion des risques.

Il existe diverses normes et cadres de référence pour la gestion des risques, tels que l'ISO 31000, qui fournit des lignes directrices internationales sur la gestion des risques.

En somme, la gestion des risques est un pilier fondamental de la gestion d'entreprise moderne, permettant aux organisations de naviguer avec succès dans un monde en constante évolution, tout en préservant leur stabilité, leur rentabilité et leur réputation.

Section 01 :

Aperçu sur le Risk Management

1- Généralités :

L'histoire de la gestion des risques (Risk Management) remonte à plusieurs siècles, mais son développement en tant que discipline formelle est plus récent. Voici une chronologie simplifiée des événements clés dans l'histoire du Risk Management :

1.1- Historique :

1.1.1- Antiquité :

Les premiers exemples de gestion des risques remontent à l'Antiquité. Les marchands assuraient leurs cargaisons contre les pertes en mer en répartissant les marchandises entre plusieurs navires pour minimiser les risques de perte totale.

1.1.2- Assurance maritime au Moyen Âge :

Au Moyen Âge, les marchands italiens ont développé des contrats d'assurance pour protéger leurs investissements maritimes. Ces contrats préfiguraient certains concepts clés de la gestion des risques modernes. [14]

1.1.3- Assurance-incendie au 17éme siècle :

À Londres, au XVIIe siècle, naît le concept d'assurance-incendie. Des compagnies d'assurance ont été créées pour indemniser les pertes liées aux incendies, et des inspections régulières des bâtiments ont été introduites pour évaluer les risques.

[14] The Invisible Hand: How an Insurer Thinks about Risk" par Kenneth S. Abraham.

1.1.4- Développement de l'assurance au 18e siècle :

L'assurance s'est développée au XVIIIe siècle avec la création de nombreuses compagnies d'assurance. Les compagnies d'assurance ont commencé à évaluer les risques de manière plus systématique.

1.1.5- Révolution industrielle :

Au cours de la Révolution industrielle, la gestion des risques a pris de l'importance dans les industries. Les entreprises ont commencé à examiner les risques liés à la production, à la sécurité des travailleurs et aux perturbations du marché.

1.1.6- Émergence de la gestion des risques d'entreprise (ERM) au 20e siècle :

Au 20éme siècle, la gestion des risques a évolué pour inclure une approche plus holistique, avec un accent particulier sur la gestion des risques d'entreprise (ERM). Les entreprises ont commencé à adopter des approches plus systématiques pour identifier, évaluer et gérer les risques à tous les niveaux de l'organisation.[15]

1.2- Normes et réglementations :

Au fil des décennies, des normes et des réglementations ont été développées pour encadrer la gestion des risques dans divers secteurs. Par exemple, le Comité de Bâle sur le contrôle bancaire a introduit des normes internationales pour la gestion des risques bancaires.

1.3- Évolution numérique :

Avec l'avènement de l'informatique et des technologies de l'information, la gestion des risques a également évolué. Les modèles informatiques sophistiqués, l'analyse des données et les outils logiciels ont été intégrés pour améliorer la gestion des risques.[16]

[15] Risk Management and Insurance" par Scott E. Harrington et Gregory R. Niehaus

[16] Enterprise Risk Management: From Incentives to Controls" par James Lam.

1.4- Gestion des risques dans la finance :

La crise financière de 2008 a mis en évidence l'importance cruciale de la gestion des risques dans le secteur financier. Cela a conduit à des réformes réglementaires et à un renforcement des pratiques de gestion des risques dans les institutions financières.

1.5- Le contexte normatif du Risk Management :

Le Risk Management se réfère à l'ensemble des normes, réglementations, lignes directrices et meilleures pratiques qui encadrent la manière dont les organisations gèrent les risques. Ces normes sont conçues pour aider les entreprises à identifier, évaluer, atténuer et gérer les risques qui pourraient affecter leurs activités.

Voici quelques-unes des normes et cadres les plus couramment utilisés dans le domaine du Risk Management :

1.5.1-ISO 31000 :2018 : Il s'agit de la norme internationale pour la gestion des risques. Elle fournit des lignes directrices et des principes pour la mise en place d'un cadre de gestion des risques efficace.

1.5.2-COSO Enterprise Risk Management : Publié par le Committee of Sponsoring Organizations of the Treadway Commission (COSO), ce cadre propose une approche complète de la gestion des risques en intégrant les risques au sein des processus de prise de décision de l'organisation.

1.5.3-Basel III : C'est un ensemble de normes bancaires internationales qui comprend des exigences spécifiques en matière de gestion des risques pour les institutions financières. Il met l'accent sur la gestion adéquate des risques de crédit, de marché et opérationnels. [17]

[17] Comité Basel sur la supervision Bancaire - Basel II: Convergence international sur mesure et normes de fonds propres : A version révisée.

1.5.4-Sarbanes-Oxley Act (SOX) : Cette loi américaine impose des exigences strictes en matière de gouvernance d'entreprise et de responsabilité des dirigeants. Bien qu'elle ne se concentre pas exclusivement sur la gestion des risques, elle exige la mise en place de contrôles internes efficaces pour atténuer les risques liés à la divulgation financière.

1.5.5-NIST Cybersecurity : Développé par le National Institute of Standards and Technology (NIST), ce cadre est axé sur la gestion des risques liés à la cybersécurité. Il fournit des directives pour aider les organisations à renforcer leur posture de sécurité informatique.

1.5.6-Solvabilité II : C'est un cadre réglementaire européen qui établit des normes pour la réglementation et la supervision des sociétés d'assurance. Il met l'accent sur la gestion des risques en matière d'assurance.

Ces normes aident les organisations à mettre en place des processus structurés et cohérents pour gérer les risques, à garantir la conformité aux réglementations en vigueur et à améliorer la résilience organisationnelle. Il est important pour les entreprises de comprendre et de suivre ces normes pour assurer une gestion efficace des risques et protéger la valeur à long terme de l'organisation.

La norme ISO 31000 définit le Risk Management (gestion des risques) comme étant "la coordination systématique de toutes les activités de l'organisation en matière de gestion des risques afin de réaliser des objectifs spécifiques et de soutenir la prise de décision éclairée."

La norme ISO 31000 met l'accent sur la prise de décision éclairée et la création de valeur. Elle souligne l'importance de l'intégration de la gestion des risques dans les processus organisationnels, la culture et la structure, tout en encourageant la communication et la consultation à tous les niveaux de l'organisation. L'approche préconisée par la norme est adaptable à différentes situations et permet aux organisations de s'adapter aux changements internes et externes tout en gérant efficacement les risques. [18]

[18] La Norme ISO 31000 version 2018.

2- Importance du Risk Management dans la prise de décision :

Le Risk Management, ou gestion des risques, joue un rôle crucial dans la prise de décision au sein des organisations. Voici quelques points clés illustrant son importance :

2.1- Anticipation des risques : Le Risk Management permet d'anticiper les risques auxquels une organisation pourrait être confrontée. En identifiant ces risques à un stade précoce, les décideurs sont mieux préparés à les gérer efficacement.

2.2- Prise de décision éclairée : En évaluant et en comprenant les risques associés à différentes options, les décideurs peuvent prendre des décisions plus éclairées. Cela contribue à minimiser l'incertitude et à accroître la probabilité de succès des initiatives.

2.3- Optimisation des ressources : La gestion des risques permet d'allouer les ressources de manière plus efficace. En identifiant les risques, les décideurs peuvent hiérarchiser les priorités et allouer les ressources là où elles sont le plus nécessaires pour atténuer les risques.

2.4- Protection de la réputation : Certains risques peuvent avoir un impact significatif sur la réputation d'une organisation. Une gestion proactive des risques permet de minimiser ces impacts négatifs et de protéger la réputation de l'entreprise.

2.5- Conformité réglementaire : Dans de nombreux secteurs, il est essentiel de se conformer à des réglementations strictes. La gestion des risques aide les organisations à identifier les risques de non-conformité et à mettre en place des mesures correctives pour éviter des sanctions et des conséquences juridiques.

2.6- Réduction des pertes financières : Les risques sont souvent liés à des pertes financières potentielles. La gestion des risques vise à minimiser ces pertes en mettant en place des stratégies d'atténuation et des plans de continuité des activités.

2.7- Planification stratégique : En intégrant la gestion des risques dans la planification stratégique, les décideurs peuvent élaborer des stratégies plus robustes et résilientes. Cela favorise une vision à long terme et une meilleure adaptation aux changements de l'environnement commercial.

2.8- Amélioration de la réactivité : En comprenant les risques, les organisations sont mieux préparées à réagir rapidement en cas de situation critique. Cela peut minimiser les dommages et accélérer le processus de récupération.

En effet, le Risk Management fournit une perspective holistique des risques auxquels une organisation est confrontée et offre des outils pour les gérer de manière proactive. Intégrer la gestion des risques dans le processus de prise de décision contribue à renforcer la résilience organisationnelle et à maximiser les chances de réussite.

3- Objectif du Risk Management :

L'ISO 31000 est une norme internationale qui fournit des lignes directrices pour la gestion des risques dans les organisations. L'objectif principal du Risk Management (gestion des risques) selon la norme ISO 31000 est d'aider les organisations à atteindre leurs objectifs en identifiant, évaluant et gérant de manière proactive les risques. Voici quelques-uns des principaux objectifs du Risk Management selon l'ISO 31000 :[19]

3.1- Intégration dans la gouvernance et la culture de l'organisation : L'ISO 31000 encourage l'intégration de la gestion des risques dans la gouvernance globale de l'organisation et dans sa culture. La gestion des risques doit être alignée sur les objectifs stratégiques et les valeurs de l'organisation.

3.2- Prise de décision éclairée : La norme vise à fournir aux dirigeants et aux décideurs des informations pertinentes sur les risques afin de les aider à prendre des décisions éclairées. Cela implique l'identification des risques, l'évaluation de leur impact potentiel et la mise en place de stratégies de gestion appropriées.

[19] La Norme ISO 31000 version 2018.

3.3- Amélioration de la performance : La gestion des risques selon l'ISO 31000 vise à contribuer à l'amélioration de la performance globale de l'organisation en minimisant les surprises indésirables et en maximisant les opportunités positives.

3.4- Établissement d'un processus continu : La norme encourage la mise en place d'un processus continu et itératif de gestion des risques. Cela signifie que la gestion des risques n'est pas un événement ponctuel, mais plutôt un processus qui s'intègre dans les activités quotidiennes de l'organisation.

3.5- Adaptabilité et flexibilité : La gestion des risques selon l'ISO 31000 doit être adaptée à la spécificité de chaque organisation. Elle encourage une approche flexible et personnalisée pour répondre aux besoins particuliers de chaque entité.

3.6- Communication et consultation : La norme met l'accent sur l'importance de la communication et de la consultation tout au long du processus de gestion des risques. Les parties prenantes doivent être impliquées, et une communication transparente favorise une compréhension commune des risques.

3.7- Alignement avec la stratégie : La gestion des risques doit être alignée avec la stratégie de l'organisation. Elle doit contribuer à la réalisation des objectifs stratégiques plutôt que de constituer un obstacle.

La norme ISO 31000 vise à établir une approche systématique et intégrée de la gestion des risques pour aider les organisations à anticiper, comprendre et répondre aux risques, contribuant ainsi à la réalisation de leurs objectifs.

Section 02 :

La démarche du Risk Management

La norme ISO 31000 :2018 sur le management des risques fournit un cadre pour la gestion des risques qui peut être appliqué à toute organisation, quelle que soit sa taille, sa structure ou son secteur d'activité. Le Risk Management selon la norme ISO 31000 implique une approche proactive et intégrée pour identifier, évaluer, gérer et surveiller les risques de manière continue dans le but d'atteindre les objectifs de l'organisation.

1- Cadre de la gestion des risques :

La norme ISO 31000 est une norme internationale qui établit des lignes directrices pour la gestion des risques dans les organisations. Elle offre un cadre complet pour aider les organisations à concevoir, mettre en œuvre, surveiller et améliorer leur processus de gestion des risques.

La norme recommande l'établissement d'un cadre de gestion des risques, qui définit les responsabilités, les processus, les politiques et les procédures pour la gestion des risques au sein de l'organisation. Ce cadre doit être intégré à la stratégie globale de l'organisation.

1.1- Contexte de l'organisation :

Avant d'entreprendre l'évaluation des risques, l'organisation doit définir son contexte, y compris ses objectifs, son environnement externe et interne, ainsi que les parties prenantes concernées. [20]

1.2- Identification des risques :

Cette étape consiste à recenser tous les risques qui pourraient affecter la réalisation des objectifs de l'organisation. Il s'agit d'une démarche proactive qui peut impliquer l'analyse des processus, des activités, des parties prenantes, etc. Al'issue de cette étape, tous les risques sont formalisés dans un document appelé le « Risk Register ».

[20] "Risk Management : Concepts and Guidance",fifth edition 2015, **par Carl** L. Pritchard.Edition.

1.3- Analyse des risques :

Une fois les risques identifiés, l'organisation doit évaluer la probabilité de leur occurrence et l'impact potentiel sur les objectifs. Cela peut inclure l'utilisation de méthodes telles que l'analyse qualitative, semi-quantitative ou quantitative, en fonction des besoins et des ressources disponibles.

1.4- Évaluation des risques :

L'évaluation des risques implique de comparer les résultats de l'analyse des risques avec les critères préalablement définis. Elle peut conduire à la classification des risques en termes de niveau de gravité, de priorité ou de criticité.

1.5- Traitement des risques :

Une fois les risques évalués, l'organisation doit décider de la manière de les gérer. Les options peuvent inclure l'acceptation du risque, la mise en œuvre de mesures d'atténuation, le transfert du risque, ou même l'évitement du risque en évitant certaines activités.

1.6- Communication et consultation :

Tout au long du processus, la communication et la consultation avec les parties prenantes sont essentielles. Cela garantit que les différentes perspectives et connaissances sont prises en compte.

1.7- Surveillance et revue :

La gestion des risques est un processus continu. L'organisation doit établir des mécanismes de surveillance pour suivre l'efficacité des mesures prises, et des revues périodiques doivent être effectuées pour garantir que le processus de gestion des risques reste adapté à l'évolution de l'environnement organisationnel.

L'ISO 31000 est flexible et peut être adaptée en fonction de la taille, de la complexité et de la nature spécifique de chaque organisation. Cette norme incite une approche intégrée de la gestion des risques, intégrant la gestion des risques dans la culture et les processus de l'organisation.

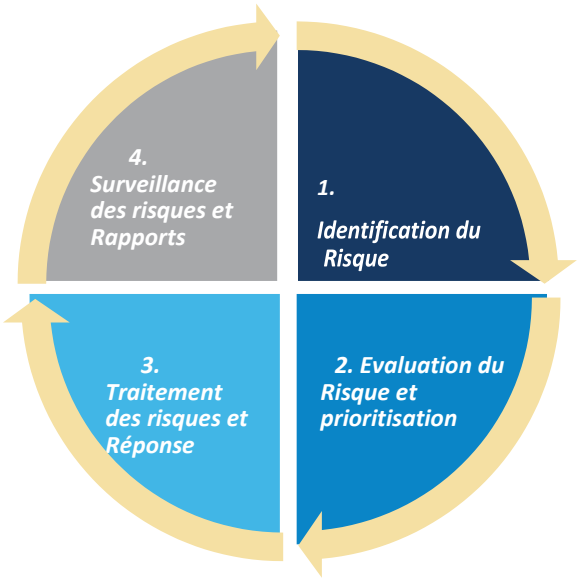


Figure n°01 : Process de gestion des risques, Source : La norme ISO 31000

2- Méthode d'analyse des risques :

L'analyse des risques est un processus essentiel dans la gestion globale des risques d'une organisation. Il vise à identifier, évaluer et atténuer les risques qui pourraient affecter les objectifs d'une entreprise. Il existe plusieurs méthodes d'analyse des risques, chacune ayant ses avantages et ses inconvénients. Voici quelques-unes des méthodes couramment utilisées :

2.1- Analyse SWOT (Force, Faiblesse, Opportunité, Menace) :

Ce type d'analyse est primordial dans toute entreprise et son utilisation est très répandue, car elle peut s'appliquer à **tous types d'entreprise**, quelle que soit la taille ou l'activité. Elle peut se réaliser de manière indépendante, pour chacun des services de l'entreprise, ou de manière globale pour l'ensemble de l'entreprise.[21]

L'analyse SWOT est divisée en deux parties principales :

- **L'analyse interne :** elle se compose des forces et des faiblesses de l'entreprise. Cette première phase permet d'analyser des points clé comme la production, les ressources humaines, le marketing ou la situation financière.

[21] Risk Management : Concepts and Guidance",fifth edition 2015, **par Carl** L. Pritchard.Edition.

- **L'analyse externe :** elle concerne les risques et les opportunités. Cette analyse prend en compte la situation du marché dans le secteur de l'entreprise, la législation en vigueur, la concurrence, les fournisseurs et l'environnement.

  - ✓ **Les forces** sont les circonstances intrinsèques à l'entreprise qui permettent d'avoir un avantage compétitif à l'égard des autres entreprises du secteur. Autrement dit, vous êtes meilleurs que les autres sur un ou plusieurs points concrets et vous devrez donc les renforcer.

  - ✓ **Les faiblesses** de l'analyse interne se rapportent aux situations ou milieux dans lesquels l'entreprise ne se débrouille pas aussi bien que ses concurrents, ou qui pourraient être améliorés. Autrement dit, les faiblesses sont tout ce qui empêche un meilleur fonctionnement de l'entreprise, mais une fois identifiées, vous ferez tout votre possible pour les éliminer.

  - ✓ **Les opportunités** représentent les avantages du secteur, comme des niches de marché qui ne sont pas encore couvertes ou une situation de marché avantageuse qui permettrait d'être meilleur que les concurrents. Il est important d'analyser le marché et la position dans laquelle se trouve votre entreprise pour trouver des avantages permettant de vous améliorer.

  - ✓ Dans **les risques**, nous retrouvons toutes les circonstances extérieures qui peuvent mettre en péril la survie de l'entreprise ou une amélioration de ses capacités. Par exemple, un secteur en crise ou un concurrent prenant beaucoup d'ampleur en peu de temps : les deux situations seraient nuisibles pour l'entreprise.[22]

[22] Risk Management : Concepts and Guidance",fifth edition 2015, **par Carl** L. Pritchard.Edition.

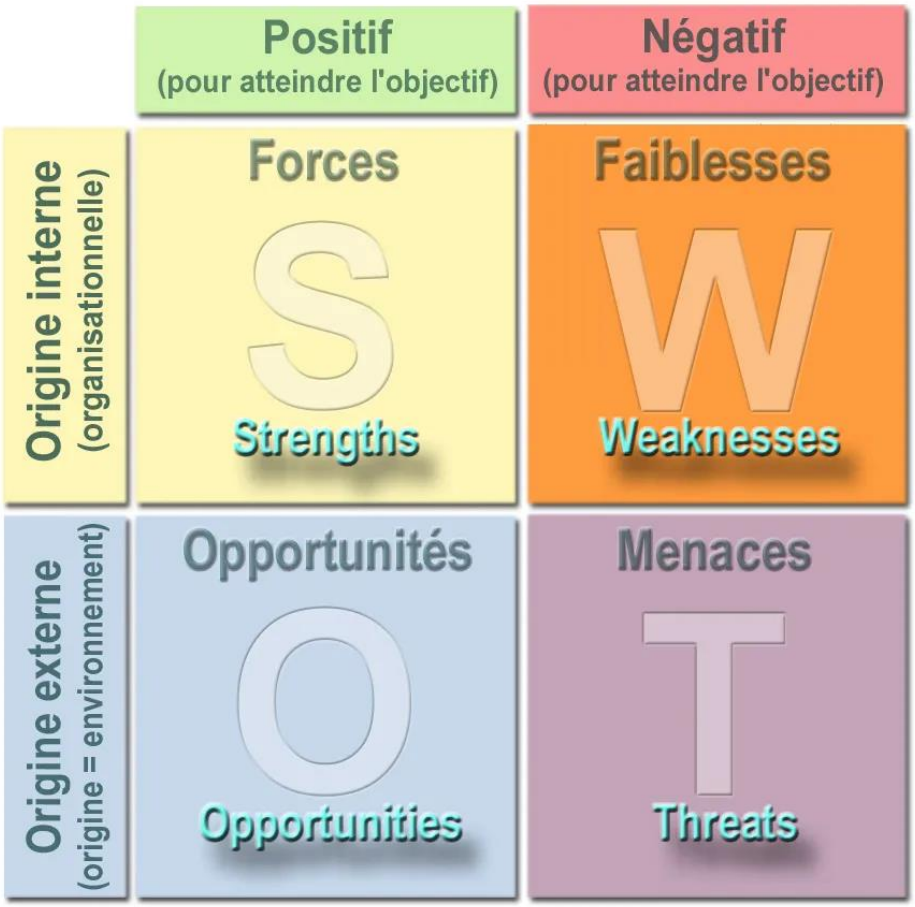


Figure n°02 : Analyse SWOT, Source : SWOT - Définition, Exemples, Processus, Utilisations (corporatefinanceinstitute.com);

2.2- Analyse des causes à effets (Diagramme d'Ishikawa ou Fishbone) :

Le diagramme causes-effets d'Ishikawa, également appelé diagramme arête de poisson, est un outil qualité utilisé pour identifier les causes d'un problème. Il sert à lister les causes qui ont une influence sur un effet (une situation), de les classer et de les hiérarchiser. Le diagramme d'Ishikawa est applicable à l'ensemble des métiers de l'entreprise.

2.3- Méthode PESTEL :

L'analyse PESTEL (ou PESTLE) est un cadre d'analyse en stratégie d'entreprise. L'acronyme, qui signifie politique, économique, sociologique, technologique, environnemental et légal, recouvre les facteurs macro-environnementaux (Externe) qui peuvent influencer (positivement ou négativement) une entreprise. L'analyse PESTEL n'est cependant pas un outil mais une aide mnémotechnique qui permet d'effectuer plus simplement une analyse externe, et ainsi de réaliser une matrice SWOT.

2.4- Analyse des modes de défaillance et de leurs effets (AMDEC) :

L'analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC) est une méthode permettant d'anticiper les défaillances potentielles des processus commerciaux et d'atténuer leur impact sur les clients. Une étude AMDEC commence généralement par une séance de brainstorming composée d'une équipe expérimentée et se termine par une nouvelle analyse des risques de défaillance après l'application d'actions correctives. En fin de compte, les AMDEC peuvent aider à prévenir les défaillances industrielles coûteuses, à améliorer la fiabilité des produits et des services, et à accroître la satisfaction des clients.

2.5- Analyse des 5P :

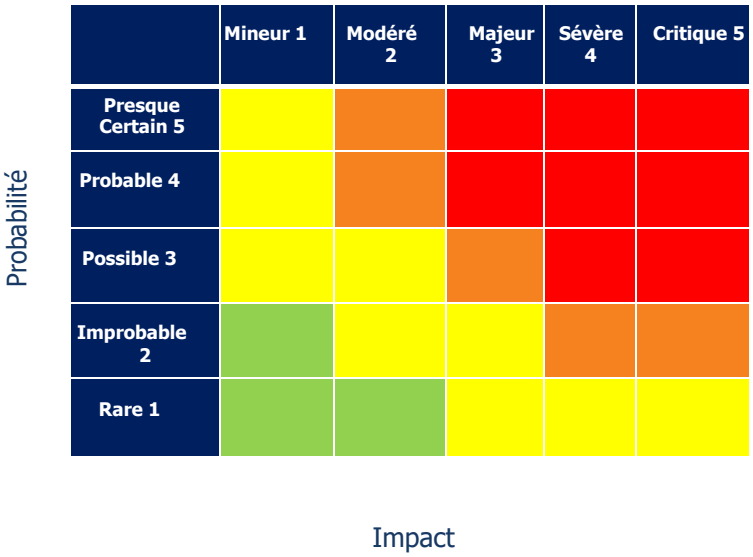
Les 5 Pourquoi servent à identifier la cause racine du dysfonctionnement grâce à l'exploration de relations directes de cause à effet. Il s'agit d'un outil qui permet d'aider à réaliser une analyse des causes et des effets.

En effet, le choix de la méthode dépend souvent du contexte spécifique de l'organisation, du projet ou de l'activité concernée. De nombreuses organisations utilisent une combinaison de ces méthodes pour obtenir une évaluation complète des risques de manière systématique, contribuant ainsi à une amélioration continue de leurs processus et de leurs performances globales.

2.6- Cartographie des Risques

La cartographie des risques est une méthode systématique permettant d'identifier, évaluer et prioriser les risques auxquels une organisation peut être confrontée. La norme ISO 31000 la considère comme une composante essentielle du processus de gestion des risques. Elle contribue à renforcer la résilience de l'organisation en anticipant et en gérant proactivement les risques.

La cartographie des risques est utilisée pour visualiser et comprendre comment les risques peuvent affecter la réalisation des objectifs de l'organisation dans ce contexte. De plus, elle peut aider à communiquer efficacement sur les risques prioritaires et les actions préventives ou correctives à prendre. Elle offre également la possibilité d'évaluer de manière visuelle l'importance des risques en tenant compte de leur probabilité et de leur impact.[23]



Gravité du Risque	Action Requise
Extrême	Inacceptable, introduire immédiatement des mesures de contrôle avec une planification détaillée, une allocation des ressources et une surveillance fréquente.
Elevé	Examiner et introduire des contrôles supplémentaires pour atténuer davantage dans la mesure du possible.
Moyen	Surveiller et maintenir des mesures de contrôle strictes tout en tenant compte de l'introduction de stratégies de traitement supplémentaires si le retour sur investissement est réalisable.
Faible	Tolérable et ne nécessite qu'une surveillance permanente.

Figure n°03 : Table de criticité, Source : La norme ISO 31000

[23] **"The Essentials of Risk Management" Second edition2014, par Michel Crouhy, Dan Galai, Robert Mark.**

Après examen et analyse des processus, la direction Évalue la probabilité que chaque risque se produise et l'impact qu'il aurait sur l'organisation en utilisant la grille ci-dessus. Par la suite, cette matrice va nous aider à visualiser la probabilité par rapport à l'impact. Cela pourra aider à hiérarchiser les risques en fonction de leur gravité.

L'une des stratégies de risque suivantes peut être déployée en fonction de l'évaluation du risque :

- **Éviter/Résilier** (risque de récompense trop élevé) - Décider de ne pas poursuivre l'activité qui a introduit le risque. Soit choisir une activité alternative plus acceptable qui répond aux objectifs de l'entreprise, soit choisir une approche ou un processus alternatif qui présente moins d'exposition au risque.

- **Réduire/Traiter (rentable à gérer à l'interne) -** Mettre en œuvre une stratégie conçue pour réduire la probabilité ou les conséquences du risque à un niveau acceptable, lorsque l'évitement ou la résiliation est excessif.

- **Transfert (économique pour transférer le risque) -** Partage ou transfert du risque à une ou plusieurs autres parties, telles que l'externalisation de la gestion des actifs physiques, l'élaboration de contrats avec des fournisseurs de services ou l'assurance contre le risque. Le tiers qui accepte le risque doit être conscient et d'accord d'accepter cette obligation.

- **Accepter/tolérer (économique pour conserver le risque) -** Prendre une décision éclairée que la cote de risque est à un niveau acceptable ou que le coût du traitement l'emporte sur les avantages. Aucune autre mesure n'est prise pour traiter le risque, mais une surveillance continue est recommandée.

L'élaboration des stratégies de risque appropriées dépendra du type et de la nature du risque ainsi que des cotes d'impact et de probabilité du risque évalué. Des indications sur les moyens et les critères selon lesquels la stratégie de risque appropriée devrait être choisie sont fournies à la figure suivante :

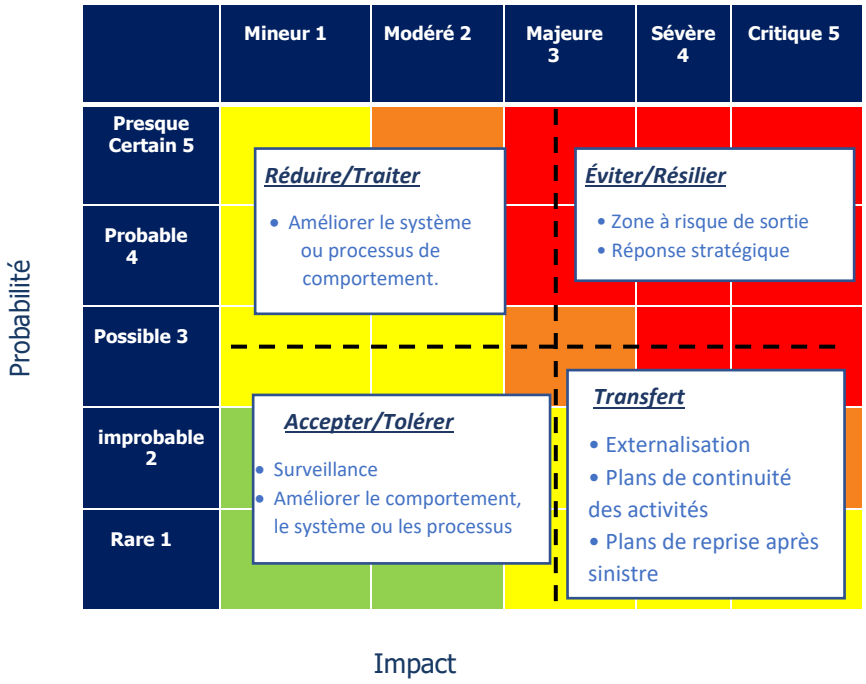


Figure N°04 : Stratégie du Risque, Source : La norme ISO 31000

3- Amélioration continue :

La norme ISO 31000 encourage les organisations à identifier et évaluer les risques de manière systématique. Ces évaluations peuvent servir de base pour l'amélioration continue en identifiant les domaines où des améliorations sont nécessaires pour réduire les risques.

Le concept d'amélioration continue consiste en un effort continu pour améliorer les produits, les services ou les processus. Les efforts peuvent viser à apporter des petites améliorations à intervalles réguliers (de façon incrémentale) ou, au contraire, à regrouper toutes les améliorations dans une implémentation globale. Les principales méthodes d'amélioration continue sont:

3.1- Roue de Deming ou PDCA

La Roue de Deming, également connue sous le nom de cycle PDCA, est un modèle de gestion itératif développé par le statisticien et consultant en gestion W. Edwards Deming. PDCA est l'acronyme de Plan-Do-Check-Act (ou Adjust). Ce modèle est largement utilisé dans le domaine de la gestion de la qualité, de l'amélioration continue des processus et de la résolution de problèmes.

Les quatre étapes du cycle PDCA sont les suivantes :

1. **Plan (Planifier) :** Définir l'objectif du processus ou du projet, identifier les méthodes pour atteindre cet objectif, planifier les ressources nécessaires et définir des critères de mesure pour évaluer les résultats.
2. **Do (Faire) :** Mettre en œuvre le plan. Cela implique l'exécution des actions planifiées. C'est la phase de mise en œuvre où les processus sont mis en pratique.
3. **Check (Vérifier) :** Évaluer les résultats obtenus par rapport aux objectifs fixés. Cela implique la collecte de données et la comparaison des résultats réels avec les résultats attendus.
4. **Act (Agir) :** Prendre des mesures basées sur l'évaluation des résultats. Si les résultats ne sont pas conformes aux attentes, cette étape implique des ajustements, des corrections et des améliorations pour atteindre les objectifs fixés. Si les résultats sont satisfaisants, les actions sont standardisées pour être répétées lors des prochaines itérations.

Le cycle PDCA encourage une approche itérative et continue de l'amélioration des processus. Il est conçu pour favoriser l'apprentissage organisationnel et l'adaptabilité en intégrant la rétroaction continue dans le processus de gestion. Ce modèle a été largement adopté dans les entreprises et les organisations du monde entier pour améliorer la qualité, l'efficacité opérationnelle et la résolution de problèmes.

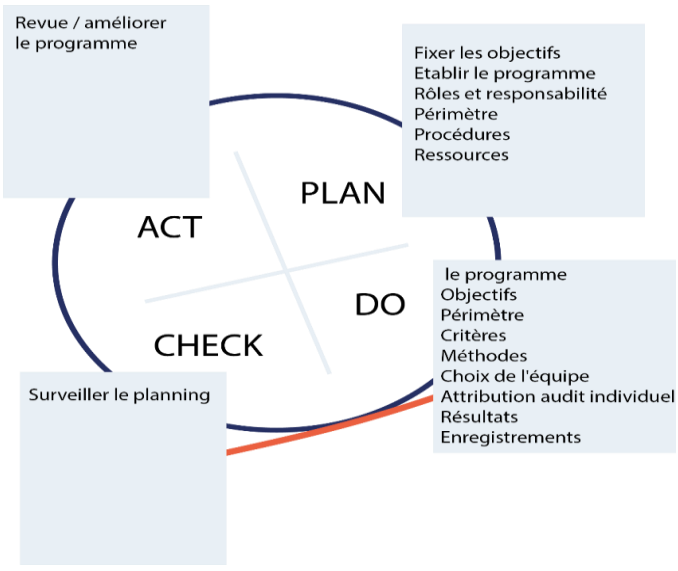


Figure N°05 : Roue de Deming, Source : La roue de Deming.pdf notice & manuel d'utilisation.

3.2- Lean Management

Le Lean Management, également connu sous le nom de Lean Manufacturing ou simplement Lean, est une approche de gestion qui vise à maximiser la valeur pour le client tout en minimisant le gaspillage. Cette philosophie a émergé à partir des pratiques de production développées par Toyota dans les années 1950 et est devenue depuis un concept clé dans le domaine de la gestion et de l'amélioration des processus.[24]

Voici quelques principes fondamentaux du Lean Management :

1. **Élimination des gaspillages :** Le Lean se concentre sur l'identification et l'élimination des activités qui n'ajoutent pas de valeur au produit ou au service final. Les sept types de gaspillages identifiés dans le Lean sont le transport, l'inventaire, le mouvement, l'attente, la surproduction, la surprocessus et les défauts.
2. **Amélioration continue (Kaizen) :** Le Lean promeut une culture d'amélioration continue. Les processus sont constamment évalués et ajustés pour accroître l'efficacité et la qualité.
3. **Production tirée par la demande :** Au lieu de produire en excès et de stocker des inventaires importants, le Lean encourage la production basée sur la demande réelle du client. Cela réduit les coûts associés à la surproduction et minimise les risques liés aux changements de demande.
4. **Flexibilité et réactivité :** Les organisations Lean sont conçues pour être flexibles et réactives aux changements dans l'environnement commercial. Cela inclut la capacité à ajuster rapidement la production en fonction des besoins du marché.
5. **Engagement des employés :** Le Lean Management valorise la participation active des employés à l'amélioration des processus. Les travailleurs sont encouragés à signaler les problèmes et à contribuer à la résolution des défis opérationnels.
6. **Juste-à-temps (JIT) :** Le système Juste-à-temps, un concept clé du Lean, vise à produire ce dont le client a besoin, au moment où il en a besoin, et en la quantité requise.

L'application du Lean Management n'est pas limitée à la fabrication. Elle peut être étendue à d'autres secteurs tels que les services, la santé, et même la gestion de projet. L'objectif ultime est d'optimiser les processus pour fournir une valeur maximale avec un minimum de gaspillage.

3.3- Démarche Kaizen

24 Lean Thinking : bannissez le gaspillage et créez de la richesse dans votre entreprise,Janvier 1996,Journal de la Société de recherche opérationnelle

La démarche Kaizen est une philosophie d'amélioration continue qui trouve son origine au Japon. "Kaizen" est un terme japonais qui signifie "changement positif" ou "amélioration continue". Cette approche met l'accent sur la réalisation de petits changements progressifs dans les processus et les pratiques, avec l'idée que ces améliorations cumulatives conduiront à des gains significatifs sur le long terme. La démarche Kaizen est souvent associée au Lean Management, mais elle peut être appliquée dans divers contextes, y compris la gestion de projet, la production, les opérations, et même la vie quotidienne.

Voici les principaux aspects de la démarche Kaizen :

1. **Engagement de tous les niveaux :** Kaizen implique l'engagement actif de tous les membres de l'organisation, des employés de base aux dirigeants. Tout le monde est encouragé à contribuer à l'amélioration continue.

2. **Identification des opportunités d'amélioration :** Les équipes Kaizen sont constamment à la recherche d'opportunités d'amélioration. Cela peut inclure l'observation des processus, la collecte de données, la rétroaction des employés, et l'analyse des performances.

3. **Améliorations incrémentales :** Plutôt que de rechercher des changements radicaux, la démarche Kaizen se concentre sur des améliorations incrémentales et réalisables. Cela peut inclure l'optimisation des processus, la simplification des tâches, la réduction des gaspillages, etc.

4. **Implémentation rapide :** Les changements identifiés sont mis en œuvre rapidement. Kaizen favorise une approche de "test and learn", où les ajustements sont introduits, évalués, et modifiés au besoin.

5. **Cercles Kaizen :** Dans de nombreuses organisations, des équipes appelées "Cercles Kaizen" sont formées. Ces groupes travaillent sur des problèmes spécifiques et recherchent des solutions d'amélioration.[25]
6. **Standardisation des meilleures pratiques :** Une fois qu'une amélioration a prouvé son efficacité, elle est documentée et standardisée. Cela permet d'assurer la pérennité des gains obtenus.

[25] "Kaizen: The Key to Japan's Competitive Success"par Masaaki Imai,edition McGraw-Hill Education,1986.

7. **Culture de la remise en question :** Kaizen encourage une culture où les employés sont encouragés à remettre en question le statu et à chercher constamment des moyens de faire mieux.

La démarche Kaizen repose sur la conviction que des améliorations continues, même modestes, peuvent avoir un impact significatif sur la qualité, l'efficacité et la satisfaction du client. Elle s'intègre bien avec d'autres approches de gestion telles que le Lean Management et le PDCA.

3.4- Méthode des 6 Sigma

La méthode des 6 Sigma (Six Sigma) est une approche de gestion de la qualité et de l'amélioration des processus qui vise à réduire la variabilité et à éliminer les défauts ou les erreurs. Elle repose sur des principes statistiques et est souvent utilisée pour améliorer l'efficacité opérationnelle, réduire les coûts et améliorer la satisfaction client. Le terme "Six Sigma" fait référence à un niveau de performance où la probabilité d'avoir un défaut est extrêmement faible, soit environ 3,4 défauts par million d'opportunités.[26]

Voici quelques principes clés de la méthode des 6 Sigma :

1. **Définition, Mesure, Analyse, Amélioration, Contrôle (DMAIC) :**

   La méthodologie DMAIC est au cœur de la méthode des 6 Sigma. Il s'agit d'un cycle en cinq étapes qui guide le processus d'amélioration continue. Les étapes sont les suivantes :

   - ✓ **Définition (Define) :** Identifier le problème, définir les objectifs du projet et établir les attentes des clients.
   - ✓ **Mesure (Measure) :** Collecter des données pertinentes sur le processus pour évaluer la performance actuelle et identifier les opportunités d'amélioration.
   - ✓ **Analyse (Analyse) :** Analyser les données pour identifier les causes racines des problèmes et comprendre les sources de variabilité dans le processus.
   - ✓ **Amélioration (Improve) :** Mettre en œuvre des solutions pour résoudre les problèmes identifiés et améliorer le processus.
   - ✓ **Contrôle (Control) :** Établir des mesures de contrôle pour maintenir les améliorations et s'assurer que le processus reste stable.

[26] **"The Toyota Way: 14 Management Principles from the World's Greatest Manufacturer" par Jeffrey K. Like,edition 2003.**

2. **Utilisation d'outils statistiques :** La méthode des 6 Sigma repose sur l'utilisation intensive d'outils statistiques pour analyser les données et prendre des décisions basées sur des faits. Certains outils couramment utilisés comprennent les cartes de contrôle, les analyses de régression, les analyses de variance, etc.

3. **Formation et certification :** Les praticiens de la méthode des 6 Sigma, appelés "Ceintures", suivent des formations spécifiques et obtiennent des certifications selon leur niveau d'expertise (Ceinture Blanche, Jaune, Verte, Noire, et parfois Maître Ceinture Noire).

4. **Orientation vers les résultats financiers :** La méthode des 6 Sigma est souvent alignée sur les objectifs financiers de l'entreprise, cherchant à maximiser le rendement sur investissement par le biais d'améliorations de processus.

5. **Mesure de la performance :** L'utilisation de métriques clés est cruciale dans la méthode des 6 Sigma. La performance du processus est mesurée de manière quantitative pour évaluer les gains obtenus.

La méthode des 6 Sigma a été largement adoptée dans de nombreuses industries, y compris la fabrication, les services financiers, la santé, et d'autres, en raison de son approche structurée et axée sur les données pour l'amélioration continue.

3.5- Les 7S de Mckinsey

Les 7S de McKinsey est un modèle de gestion qui a été développé par le cabinet de conseil McKinsey & Company dans les années 1980. Ce modèle est conçu pour aider les organisations à analyser et à optimiser différents aspects de leur fonctionnement. Les 7S représentent sept éléments clés qui, selon McKinsey, sont interconnectés et doivent être alignés pour assurer le succès organisationnel. Voici les sept éléments des 7S de McKinsey :

1. **Stratégie (Strategy) :** Il s'agit des actions à long terme d'une organisation pour atteindre ses objectifs. La stratégie définit la direction générale de l'entreprise.
2. **Structure (Structure) :** La structure organisationnelle, qui comprend la manière dont les différentes unités, départements et équipes sont organisés et hiérarchisés.

3. **Systèmes (Systems) :** Les systèmes représentent les processus et les procédures internes qui soutiennent le fonctionnement de l'organisation. Cela peut inclure les systèmes d'information, les processus opérationnels, les systèmes de gestion de la performance, etc.
4. **Style (Style) :** Il s'agit du style de gestion et de leadership prévalant dans l'organisation. Le style de direction influence la culture organisationnelle et a un impact sur la façon dont les employés interagissent et travaillent ensemble.
5. **Personnel (Staff) :** Les personnes, ou le personnel, représentent les compétences, les talents et les capacités des membres de l'organisation. Il est essentiel que le personnel soit aligné sur la stratégie et la structure de l'entreprise.
6. **Compétences (Skills) :** Les compétences se rapportent aux compétences spécifiques nécessaires pour mettre en œuvre la stratégie de l'entreprise. Cela peut inclure des compétences techniques, des compétences en leadership, des compétences relationnelles, etc.
7. **Valeurs partagées (Shared Values) :** Les valeurs partagées représentent les croyances et les principes fondamentaux qui guident le comportement et la prise de décision au sein de l'organisation. Les valeurs partagées sont souvent au cœur de la culture organisationnelle.

L'idée derrière les 7S de McKinsey est que tous ces éléments sont interconnectés, et pour que l'organisation fonctionne efficacement, ils doivent être cohérents et alignés les uns sur les autres. Si l'un de ces éléments est en désaccord avec les autres, cela peut entraîner des inefficacités et des dysfonctionnements au sein de l'organisation. L'utilisation du modèle des 7S peut aider les entreprises à diagnostiquer leur situation actuelle, à identifier les lacunes potentielles et à prendre des mesures pour assurer un alignement optimal.

En résumé, le cycle d'amélioration continue peut-être décrit ci-dessous :

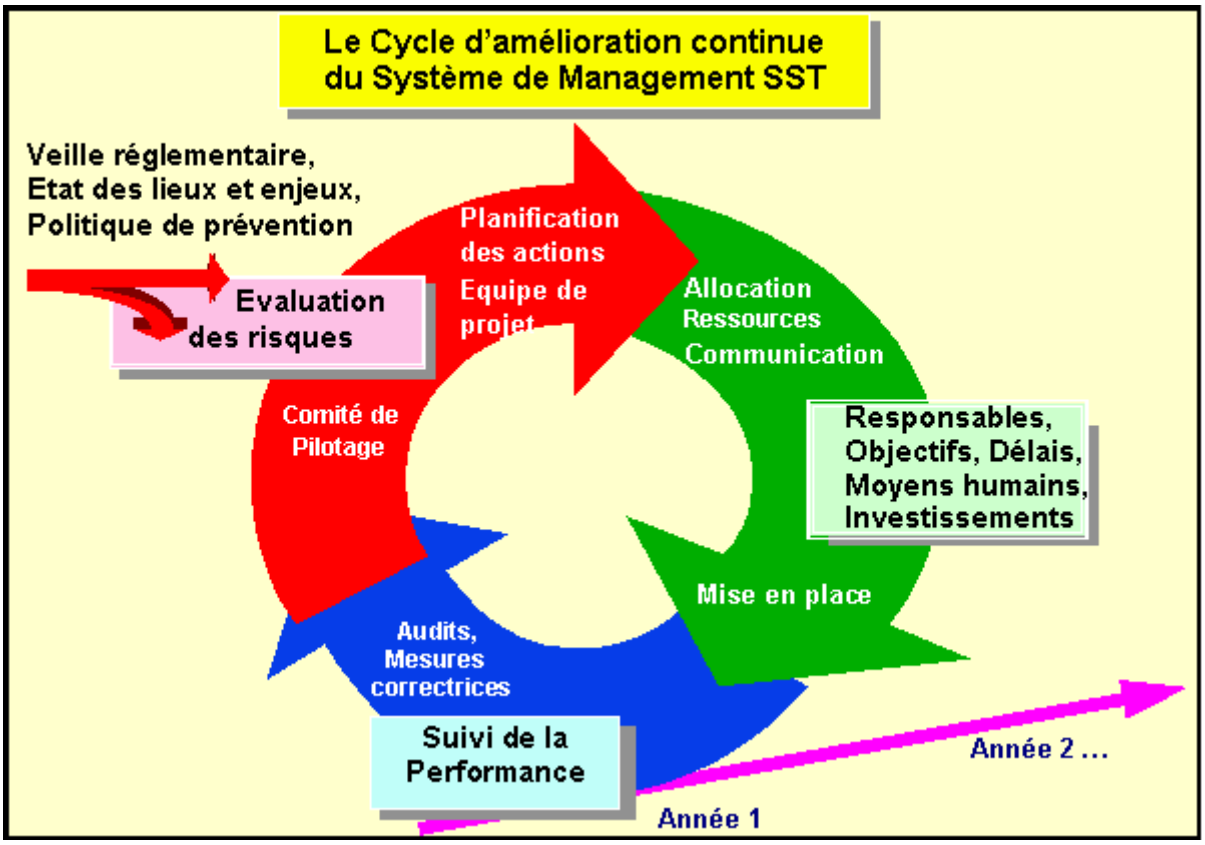


Figure N°06 : Le cycle d'amélioration, Source : La roue de Deming.pdf notice & manuel d'utilisation.

Section 03 :

Intégration du Risk Management dans la gestion d'entreprise

1- Incorporation du Risk Management dans la planification[27] :

1.1- Élaboration de scénarios :

Cela consiste à envisagez différents scénarios en fonction des risques identifiés. Développez des plans d'action spécifiques pour faire face à chaque scénario potentiel. Cependant, les détails spécifiques des plans d'action dépendront des risques spécifiques que vous avez identifiés dans votre contexte particulier. Néanmoins, ci-dessous des exemples pour vous donner une idée de la manière dont vous pourriez élaborer ces processus.

Scénario 1 : Cyberattaque

Risque identifié : Attaque de cybercriminalité entraînant un accès non autorisé à des informations sensibles.

Plan d'action :

1. Mettre en place des pares-feux et des systèmes de détection d'intrusion pour prévenir les attaques.
2. Sensibiliser les employés à la sécurité en ligne par le biais de formations régulières.
3. Effectuer des audits de sécurité réguliers pour identifier et corriger les vulnérabilités.
4. Élaborer un plan de réponse aux incidents en cas de violation de la sécurité.
5. Sauvegarder régulièrement les données importantes et stocker les sauvegardes hors ligne.

[27] **"Implementing Enterprise Risk Management: Case Studies and Best Practices" par John Fraser et Betty J. Simkins,edition :Wiley, 2014.**

Scénario 2 : Catastrophe naturelle

Risque identifié : Catastrophe naturelle telle qu'un tremblement de terre, une inondation ou une tempête.

Plan d'action :

1. Élaborer un plan d'évacuation clair pour les employés.
2. Mettre en place des protocoles de communication d'urgence.
3. Stocker des fournitures d'urgence telles que des trousses de premiers soins, des lampes de poche et de la nourriture non périssable.
4. Assurer la sauvegarde hors site des données cruciales.
5. Établir des partenariats avec des services d'urgence locaux.

Scénario 3 : Pandémie

Risque identifié : Épidémie mondiale affectant la santé des employés et perturbant les opérations commerciales.

Plan d'action :

1. Mettre en œuvre des politiques de travail à distance et fournir les ressources nécessaires.
2. Mettre en place des protocoles de désinfection et de distanciation sociale sur le lieu de travail.
3. S'assurer que les employés sont informés des pratiques d'hygiène et de sécurité.
4. Établir des plans de continuité des activités pour maintenir les opérations essentielles.
5. Collaborer avec les autorités sanitaires locales.

Ces plans d'action sont génériques et doivent être adaptés en fonction de la nature spécifique de l'entreprise, du secteur d'activité et des risques identifiés. Il est également essentiel de réviser et de mettre à jour régulièrement ces plans pour refléter les changements dans votre environnement opérationnel.

1.2- Intégration dans la planification stratégique :

Après avoir identifié des scénarios pour différents type de risque. Il est nécessaire d'identifier les conséquences possibles de chaque scénario sur la réalisation des objectifs stratégiques.

Ensuite intégrer ces scénarios dans la planification stratégique, et cette étape consiste particulièrement à réviser les objectifs à long terme en tenant compte des résultats de l'évaluation des risques. Il est important aussi de s'assurer que les objectifs sont réalistes et tiennent compte des défis potentiels.

1.3- Planification opérationnelle :

Il s'agit d'utiliser une matrice de risques pour classer les risques en fonction de leur probabilité et de leur impact. Identifiez les risques opérationnels prioritaires nécessitant une attention immédiate.

Incluez des plans d'action spécifiques et adapter pour atténuer, transférer ou accepter les risques identifiés dans la planification opérationnelle. S'assurer que chaque membre de l'équipe comprend son rôle et sa responsabilité dans la gestion des risques.

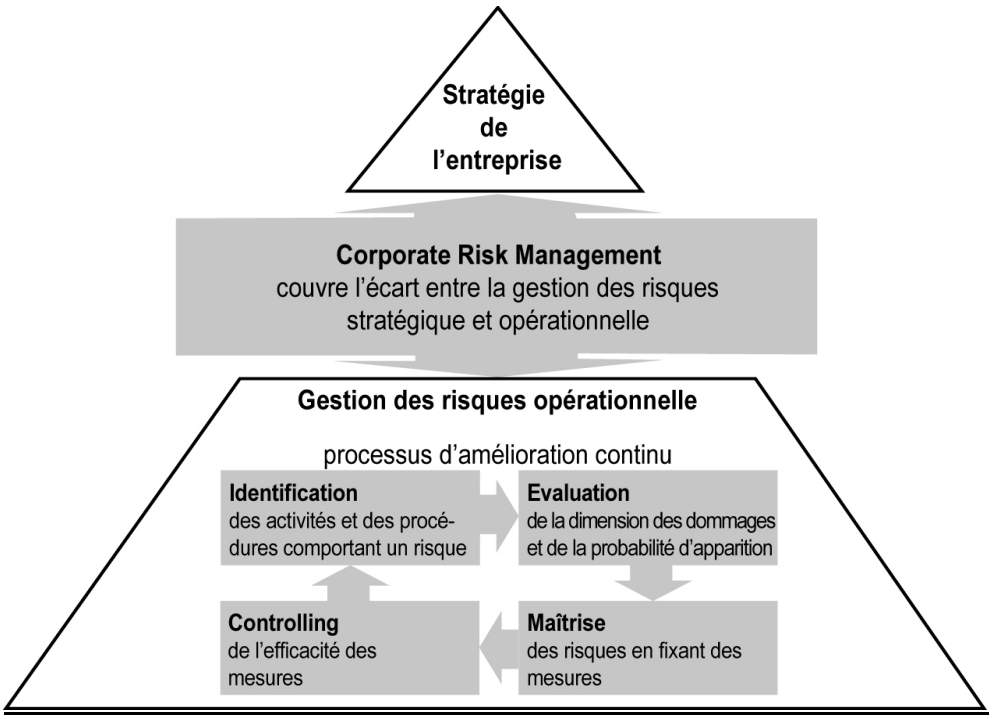


Figure N°07 :Incorporation de la gestion des risques dans la stratégique de l'entreprise , Source : Gestion des risque opérationnelle Images (bing.com)

1.4- Mise en œuvre des plans de gestion des risques :

La mise en œuvre des plans de gestion des risques requière d'appliquer de manière proactive les plans de gestion des risques, et de les adapter au besoin et vérifier l'efficacité des mesures d'atténuation. Ainsi, d'effectuer des tests pilotes pour évaluer ces mesures, et recueillir des retours d'expérience après leur mise en œuvre pour identifier les points forts et faibles. Cela va faciliter la détermination des ressources requises pour la mise en œuvre des plans d'action liés à la gestion des risques, puis allouez des ressources humaines, financières et matérielles spécifiques à chaque plan d'action.[28]

[28] "The Risk Management Process : Business Strategy and Tactics" par Christopher L. Culp, Edition Wiley 2001.

Il s'agit également de développer des plans de réponse aux risques qui détaillent les actions spécifiques à entreprendre en cas de réalisation d'un scénario de risque. Ces actions peuvent inclure des mesures d'atténuation, des plans d'urgence, ou des ajustements de la stratégie en cours de route.

2- Surveillance continue des risques :

Il s'agit de mettre en place un système de suivi en permanence des risques pour surveiller l'efficacité des stratégies de gestion des risques. Cela consiste à :

- ✓ Etablir un processus et un mécanisme de surveillance continue pour évaluer l'efficacité des mesures d'atténuation et pour identifier de nouveaux risques, tels que des rapports périodiques, des revues de performance et des audits, pour identifier les changements dans le paysage des risques.

- ✓ Prévoir des révisions périodiques du plan en tenant compte des nouvelles informations, des changements réglementaires, et du contexte en général.

- ✓ Ajuster la stratégie de chaque risque au besoin.

- ✓ Révision régulière avec l'équipe de gestion des risques, par exemple :

    - Convoquez des réunions régulières avec l'équipe de gestion des risques pour discuter des progrès, des ajustements nécessaires et des anciennes expériences apprises.

    - Encouragez l'équipe à rester proactive dans son approche de gestion des risques.

3- Communication efficace sur les risques :

3.1- Communication interne :

Assurer une communication transparente au sein de l'organisation pour informer les parties prenantes des risques identifiés, des plans d'atténuation et des responsabilités.

3.2- Communication externe :

Lorsque les risques ont le potentiel d'affecter des parties externes (clients, partenaires, actionnaires, etc.), une communication proactive est nécessaire pour minimiser l'impact perçu.

3.3- Élaboration de messages clés :

Identifier les messages clés à communiquer pour assurer une compréhension claire des risques et des mesures prises pour les gérer.

3.4- Adaptation du langage :

Utiliser un langage adapté au public cible pour éviter la confusion et garantir une compréhension claire des enjeux.

3.6- Canal de communication approprié :

Choisir le bon canal de communication en fonction de la nature du risque et de la cible (par exemple, réunions, communiqués de presse, médias sociaux, etc.).

Communiquez de manière transparente à toutes les parties prenantes sur les risques identifiés, les plans d'action correspondants, et les ajustements nécessaires. Informez les parties prenantes des modifications apportées au plan initial en raison de l'identification des risques, et partagez les stratégies de gestion des risques, expliquant comment elles seront intégrées dans l'ensemble du processus.[29]

Favorisez la communication ouverte et encouragez les membres de l'équipe à signaler tout nouveau risque. Assurez-vous que les informations concernant les risques, les plans d'atténuation et les ajustements sont communiquées de manière claire à toutes les parties prenantes, et encouragez une communication ouverte et transparente pour renforcer la confiance au sein de l'équipe.

[29] **"La revue Communication et gestion des risques" par Vincent Gautrais et Yann Jodoin, professeurs titulaires à la Faculté de droit de l'Université de Montréal.**

Conclusion du chapitre :

En conclusion, à travers ce chapitre 2, nous avons exploré les diverses facettes du management des risques, mettant en lumière l'importance de l'anticipation, de la planification et de la réactivité face aux incertitudes.

En conclusion, il est impératif pour les organisations de développer une culture proactive de gestion des risques, intégrant des processus robustes et des outils efficaces pour anticiper et gérer les menaces potentielles.

En investissant dans une approche holistique du Risk Management, les entreprises peuvent non seulement minimiser les perturbations, mais également identifier des opportunités cachées et renforcer leur résilience face à un environnement en constante évolution.

La gestion des risques devrait être perçue comme une stratégie proactive plutôt que réactive, offrant ainsi une base solide pour la prise de décision éclairée et la réalisation réussie des objectifs organisationnels.

Chapitre 03 :
Cas pratique (Cas : de la filiale Algérienne D)

Introduction

Dans les deux chapitres antérieurs, nous avons examiné de manière approfondie les éléments clés de l'Audit interne et de la gestion des risques. Notre étude de cas se concentre sur l'audit de l'outil de gestion des risques au sein de la filiale algérienne "DA". En mettant en évidence les défis potentiels et en identifiant les opportunités d'amélioration, ce cas pratique offre une perspective concrète des procédures d'audit nécessaires pour garantir l'efficacité et la pertinence de la gestion des risques dans le contexte de la conformité à la norme "Certification ISO 28000 :2007".

La première section, "Présentation de la filiale algérienne DA", se concentrera sur une analyse approfondie de la filiale où notre étude de cas a été menée. Nous décrirons les caractéristiques de l'entreprise, notamment ses activités, son organigramme et les responsabilités de chaque département.

La deuxième section, "Audit interne du département de la sécurité", impliquera une évaluation détaillée du département de la sécurité en se basant sur les politiques, les procédures et l'ensemble du dispositif mis en place. Nous mettrons également l'accent sur les résultats de l'audit groupe préalablement réalisé. Des recommandations appropriées seront formulées pour atténuer les risques et/ou les non-conformités.

La troisième section se concentrera sur l'audit externe de conformité et/ou de certification, se focalisant sur le processus de sécurité interne. Nous assisterons le cabinet externe dans sa démarche de certification.

Section 01 :

Présentation de la cible

La filiale Algérienne « D » est un acteur majeur du transport et de la logistique en Algérie et joue un rôle essentiel dans la satisfaction des besoins des entreprises, et des particuliers à l'échelle nationale.

Cette section vise à fournir une analyse approfondie de l'entreprise en mettant l'accent sur ses activités, son historique et son organisation, tout en abordant les points clés pour la présenter de manière exhaustive.

1- Historique

Le Groupe « D » est une entreprise mondiale spécialisée dans les services et la logistique. Fondé en 1999, il est l'un des principaux acteurs du secteur de la logistique et de la chaîne d'approvisionnement à l'échelle mondiale.

Le Groupe « D » gère et exploite un vaste réseau de transport et d'infrastructures liées au commerce international. Il opère dans +93 pays (dont celui d'Alger), à travers les six continents, ses services incluent la manutention, la logistique, le transport, la distribution et d'autres services liés au commerce international.

La filiale Algérienne « D » a été créé en 2009, il s'agit d'une installation spécialisée, elle détient une part de marché en 2022, de 58% du marché Algérois et 26% à l'échelle nationale. Cette position prédominante a conduit à la création de 856 emplois directs et 200 emplois indirects.

Aujourd'hui plus de 80% du commerce mondiale, en progression constante, se fait à travers les ports. A cet effet, le port d'Alger se positionne dans un contexte stratégique régional, pas seulement national, parmi les ports compétitifs de la région méditerranéenne.

Sur le plan stratégique, la filiale contribue à la croissance économique et au développement du secteur à l'échelle Nationale et Internationale. Sur le plan opérationnel, le port dispose d'infrastructures portuaires optimales qui permette d'accroitre le nombre de traitement des conteneurs avec de meilleures performances et l'optimisation de la chaine logistique tout en améliorant la qualité des services.

2- Missions et objectifs :

Dans ce sens, nous allons détailler les missions et les objectifs de « La filiale Algérienne D », ainsi que les actions entreprises pour y parvenir.

2.1- Missions :

La filiale D est une entreprise spécialisée dans la logistique, elle a pour mission principale d'assurer le déplacement efficace et sécurisé des marchandises d'un point à un autre, tout en gérant de manière optimale l'ensemble des opérations logistiques associées sur sa plateforme. Ci-après quelques missions clés :

1. Assurer le déplacement physique des marchandises d'un lieu à un autre, en utilisant divers équipements en fonction des besoins du processus.
2. Gérer l'ensemble des activités liées au stockage, et la préparation des commandes.
3. Optimiser les niveaux de stocks pour assurer une disponibilité adéquate des marchandises tout en minimisant les coûts associés au stockage (déplacements/improductif mouvements).
4. Entretenir et gérer une flotte d'équipements, en assurant la maintenance régulière, le suivi des performances, la conformité réglementaire et la gestion des conducteurs.
5. Assurer la conformité aux réglementations douanières et aux normes réglementaires internationales pour faciliter le passage des marchandises à travers les frontières.
6. Utiliser des systèmes informatiques avancés pour suivre et gérer les opérations, y compris la gestion des commandes, la traçabilité des marchandises et la communication avec les parties prenantes.
7. Mettre en œuvre des stratégies visant à réduire les coûts opérationnels tout en maintenant un niveau élevé de qualité de service.
8. Garantir la sécurité des marchandises, des véhicules et du personnel, en mettant en œuvre des politiques et des procédures de sécurité robustes.
9. Fournir un service client de qualité en assurant une communication transparente, des mises à jour en temps réel sur le statut des expéditions et la résolution rapide des problèmes éventuels.

2.2- Objectifs :

Pour rester compétitive face à la concurrence qui se profile avec la dynamique du marché, « la filiale Algérienne D » a mis en place une politique qui regroupe un ensemble d'objectifs permettant de rester compétitive face à ses futurs concurrents :

1. **Optimisation des coûts :** Réduire les coûts liés au stockage et à la logistique pour améliorer la rentabilité globale de l'entreprise.

2. **Efficacité opérationnelle :** Mettre en place des processus logistiques efficaces pour assurer une livraison rapide, fiable et rentable des marchandises.

3. **Service à la clientèle :** Offrir un excellent service à la clientèle en assurant la ponctualité des livraisons, la gestion précise des stocks et une communication transparente.

4. **Expansion géographique :** Élargir la couverture géographique pour atteindre de nouveaux marchés et clients, ce qui peut impliquer l'ouverture de nouveaux entrepôts ou l'extension du réseau de transport.

5. **Innovation technologique :** Intégrer des technologies de pointe telles que la gestion électronique des stocks, la traçabilité des marchandises, etc., pour améliorer l'efficacité et la visibilité des opérations.

6. **Durabilité environnementale :** Adopter des pratiques et des technologies durables pour réduire l'impact environnemental des opérations de transport et de logistique.

7. **Conformité réglementaire :** Se conformer aux réglementations locales, nationales et internationales liées au transport de marchandises et à la logistique.

8. **Gestion de la chaîne d'approvisionnement :** Optimiser la chaîne d'approvisionnement de bout en bout, de la production à la distribution, pour garantir une efficacité maximale.

9. **Gestion des risques :** Mettre en place des plans de gestion des risques pour faire face aux imprévus tels que les retards, les pannes, les problèmes de sécurité, etc.

10. **Amélioration continue :** Instaurer une culture d'amélioration continue en évaluant régulièrement les performances, en recueillant des commentaires clients et en ajustant les processus en conséquence.

3- Organisation :

« La filiale Algérienne D » est organisée en trois niveaux de structures.

3.1- Direction Générale :

La Direction Générale est le niveau hiérarchique le plus élevé chez « La Filiale Algérienne D ». Elle se compose de quatre directions exécutives : Finance, Opérations, Commercial, HSE, Compliance, et Ressources Humaines.

3.2- Structure fonctionnelle :

La structure de « la filiale Algérienne D » comprend plusieurs départements ayant pour mission d'assurer le bon fonctionnement de l'entreprise. Cette structure est composée des directions de soutien et des directions centrales.

Les départements de cette structure sont : Département des opérations, Service facturation, Département comptabilité.

3.3- Structure opérationnelle :

La structure opérationnelle de « la filiale Algérienne D » est chargée de mener les activités principales de l'entreprise et est composée des branches principales : Ateliers,

les opérations, le planning, la sureté interne, Achats, la facturation, la comptabilité, la facturation et le service après-vente etc…..

Pour résumer ce que nous avons expliqué sur l'organisation de la « Filiale Algérienne D », ci-dessous est présenté le schéma hiérarchique de l'entreprise :

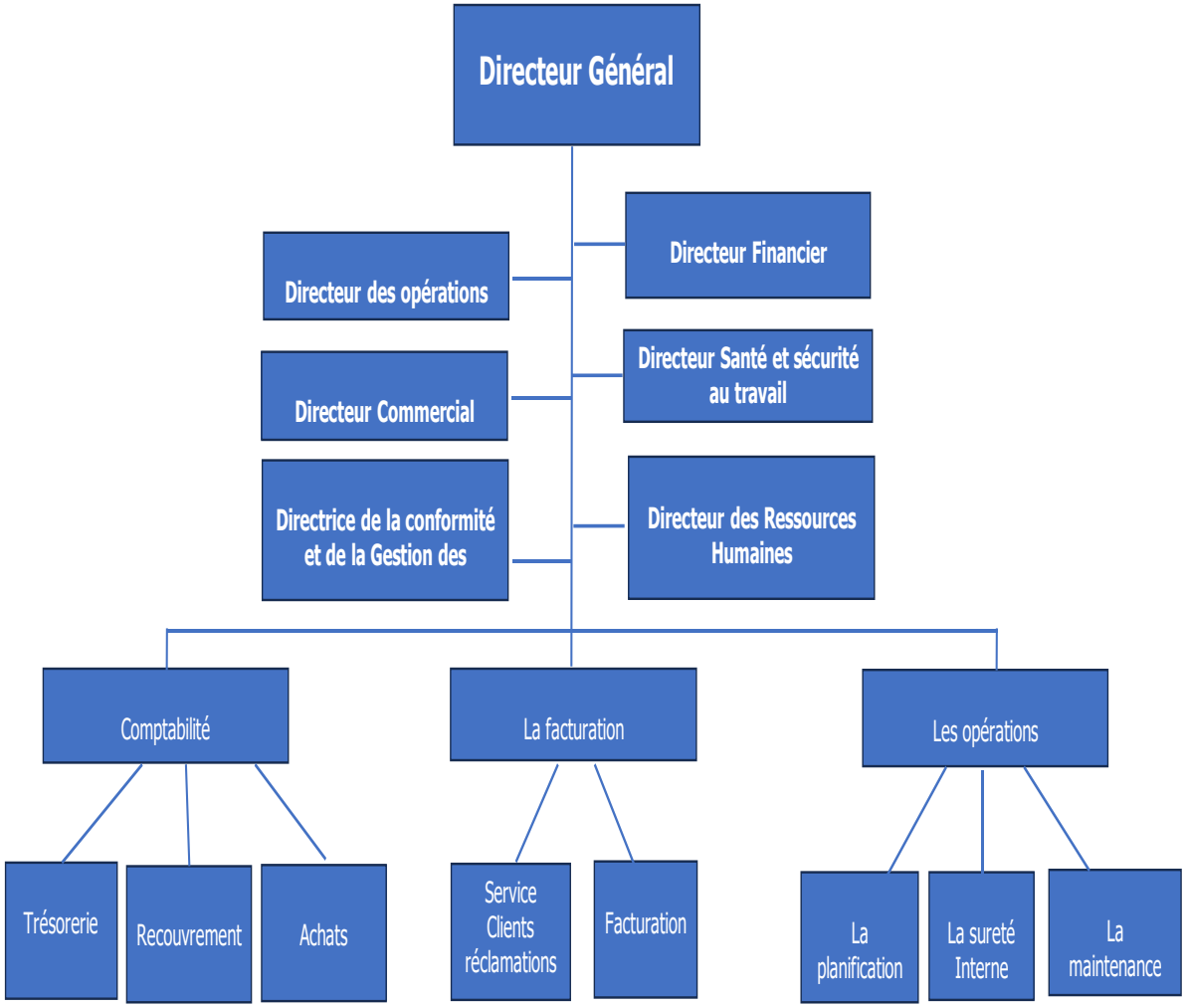


Figure N° 08: L'organigramme de la « Filiale Algérienne D »,Source : Document interne de « La Filiale Algérienne D, Exercice 2023 »;

4- Les moyens de l'entreprise :

« La filiale Algérienne D » dispose d'une capacité humaine et matérielle considérable pour accomplir ses missions, se composent de ce qui suit :

4.1- Potentiel Humain :

L'effectif employé au 31 Décembre 2023, s'élève à 873 employés, qui s'établissement comme suit :

Effectifs	Hommes	Femmes
Administration	53	29
Les opérations	696	-
Maintenance	95	-
Total	844	29
Total H/F	**873**	

Tableau 02 : L'effectif de la «Filiale Algérienne D » (Source : Documents internes, 2023)

4.2- Infrastructure :

Pour assurer sa mission, « la Filiale Algérienne D » dispose d'une infrastructure de :

- ✓ Un Bâtiment Administratif.
- ✓ Des ateliers.
- ✓ Un Bâtiment des opérations.
- ✓ Un magasin (air de stockage).
- ✓ Des cabines de sécurité.
- ✓ Dépôt des marchandises.
- ✓ Air de logistique.
- ✓ Espace Commercial et réclamations.

4.3- Potentiel matériel :

- ✓ 45 Tracteurs.
- ✓ 7 Remorques.
- ✓ 4 Grues fixes.
- ✓ 5 Grues roulantes.
- ✓ 16 Camions.
- ✓ 1 Mustang.
- ✓ 1 fourche.

5- Motivation :

Les enjeux de la sécurité sont nombreux et variés, et ils peuvent avoir des implications importantes sur la sécurité nationale, la sûreté du commerce international. Les infrastructures logistiques sont des cibles potentielles pour les actes terroristes en raison de leur importance stratégique et de leur rôle vital dans le commerce international.

La gestion efficace de ces enjeux est essentielle pour assurer la fluidité du commerce international, protéger la vie humaine, et renforcer la sécurité nationale.

Les efforts de sécurité sont souvent réglementés par des normes internationales telles que l'ISO 28000 « management de la sécurité de la chaîne d'approvisionnement ».

Par ailleurs, nous avons eu des échanges avec la Direction Générale de la filiale Algérienne « DA » et les personnes concernées dans le Groupe « D », et nous avons souligné l'importance d'aligner les objectifs de sécurité avec les objectifs la Norme internationale ISO 28000 qui permettra d'identifier, d'évaluer et de gérer de manière proactive les risques liés à la sécurité de la chaîne d'approvisionnement.

De plus, nous avons mis en avant les avantages spécifiques et pertinents de la Certification, notamment son impact sur l'amélioration de la qualité, de l'efficacité opérationnelle et de la satisfaction client.

Afin de répondre aux problématiques, il est important de réaliser une évaluation approfondie des processus actuels, des lacunes potentielles, et des besoins spécifiques de l'organisation en matière de sécurité de la chaîne logistique.

Le Risk Manager a été chargé de la mission d'évaluer le processus de sécurité actuel. Il entreprendra cette évaluation en tant que première étape en vue de l'obtention de la Certification.

Section 02 :

Audit Interne du Département de la sûreté

L'Audit Interne joue un rôle crucial dans la performance de toute entreprise, et « La Filiale Algérienne D » ne fait pas exception.

Afin de mieux comprendre l'utilité de l'Audit Interne pour le Risk Management, nous allons recourir à une mission d'Audit Interne élaboré par l'équipe interne afin d'analyser le processus de sureté et mettre en exergue le lien entre l'Audit Interne et la Gestion des Risques.

1- Objectifs de l'Audit Interne de la Sureté :

L'objectif est d'examiner l'application des procédures opérationnelles du système de gestion de la sureté actuel, conformément à la liste de contrôle ISO 28000-2007, afin d'évaluer son efficacité."

2- Scope :

"Norme ISO 28000 : 2007" ;

Article 4 : Éléments du système de gestion de la sureté (La mise en œuvre)

- ✓ 4.1 Exigences générales ;
- ✓ 4.2 Politique de gestion de la sécurité ;
- ✓ 4.3 Évaluation et planification des risques de sécurité ;
- ✓ 4.4 Mise en œuvre et exploitation ;
- ✓ 4.5 Vérification et actions correctives ;
- ✓ 4.6 Revue de direction et amélioration continue."

3- Déroulement de la mission :

L'audit interne est réalisé par le Département Conformité et Risques.

Une équipe a été sélectionnée en interne, cette équipe a suivi une méthode de formation rigoureuse en audit (Norme ISO19011 - Audit des systèmes de Management) pour garantir une mission en toute objectivité et professionnalisme.

Nom des intervenants	Fonction au sein de l'entreprise	Département	Formation ISO 19001	Fonction au sein de l'équipe
Mr C.M	IT Manager	IT	OUI	Chef de mission
Mr Z.M	HSE Manager	HSE	OUI	Auditeur
Mr B.N	Staff Control Manager	OPS	OUI	Chef de mission
Mr S.H	Senior Financial Accountant	Finance	OUI	Auditeur
Mme R.S	Coordinatrice des accès	Sureté	OUI	Guide
Mme K.R	Security assistant	Sureté	OUI	Guide
Mme K.Y	Talent & Development Supervisor	Formation	OUI	Auditrice
Mr B.S	Technical Planning Manager	Technique	OUI	Auditeur
Mme B.H	Compliance and Risk Manager	ERM	OUI	Responsable d'Audit

Tableau N°03 : La liste des intervenants (Source : élaboré par nos soins)

Notre mission s'est déroulée en trois phases :

- Phase 01 : Entretien avec le Responsable de la Sureté, ainsi qu'avec les membres de son équipe, conformément au champ de la mission ;
- Phase 02 : Collecte et examen des documents ;
- Phase 03 : Visite d'inspection pour évaluer concrètement le système de gestion mis en place.

Les activités suivantes ont été utilisées dans le cadre de notre mission :

3.1- Communication :

Une communication a été effectuée pour tous les départements lors d'une réunion d'ouverture, en présence du DG, du Directeur financier, du Directeur des opérations, du Responsable de la sécurité, du Responsable des achats, du Responsable des ressources humaines et du Responsable de la formation.

3.2- Revue documentaire :

Nous avons examiné les documents suivants :

- ✓ Les procédures opérationnelles ;
- ✓ La politique du Groupe « D » ;
- ✓ Et, les formulaires connexes.

3.3- Visites sur site :

L'équipe d'audit a effectué une visite du terminal en compagnie du Responsable de la sécurité et du Superviseur de la sécurité. Nous avons visité le bâtiment administratif, les bureaux de sécurité, la porte d'entrée, la porte de sortie, les quais, la zone d'inspection, la zone de scanner, le bâtiment des opérations, la salle de vidéosurveillance, l'atelier technique, le magasin et toutes les cabines de sécurité existantes."

3.4- Sensibilisation :

Afin d'aider le service à effectuer une transformation et/ou mise en œuvre du système de gestion de la sécurité à toutes les échelles, nous avons sensibilisé tous les agents rencontrés lors de notre visite du terminal, concernant l'application des procédures ainsi que le respect des formulaires à remplir.

3.5- Consultation :

Discussion avec le Responsable de la sécurité, le Superviseur de la sécurité, le Coordinateur d'accès, et les agents de sécurité.

3.6- Etablissement du programme d'Audit :

L'audit s'est déroulé sur la période allant du 04 au 06 Septembre 2022.

Emploi du temps	Objectif	Nom des intervenants	Fonction au sein de l'équipe
Le 04 et 05 sept 2022	Audit + Préparation du résumé	Mr C.M Mr Z.M Mr B.N Mr S.H Mme R.S Mme K.R Mme K.Y Mr B.S Mme B.H	Chef de mission Auditeur Chef de mission Auditeur Guide Guide Auditrice Auditeur Responsable d'Audit
Le 06 Sept 2022 Matin	Revue des résumés et/ou points remontés par les chefs de missions	Chacun d'entre vous doit préparer un rapport sur excel (Checklist)pour remonter les points forts, les points faibles, les non-conformités et/ou anomalies. Chaque point remonté doit etre clair, précis et bien documenté. Chaque Chef de mission doit revoir et discuter les points remontés par ses équipes. (Les guides peuvent assister aux réunions de leur équipe respective)	
Le 06 sept 2022 Après-Midi	Réunions de synthèse avec toute l'équipe	La Réunion est faite dans l'après midi, l'ensemble de l'équipe doit etre présent.	

Tableau N°04 : Le calendrier prévisionnel (Source : élaboré par nos soins)

3.7- Ressources utilisées :

- Le temps : le délai de réalisation de cet Audit était du 04 au 06 Sept 2022.
- Les équipements : Les ordinateurs, le Data show, salle de réunion, WIFI.
- Formation : Formation ISO 19011, ISO 28000 Awarness.

3.8- Analyse :

3.8.1- Préparation des Documents d'Audit :

Rassembler les documents pertinents tels que la politique de sécurité, les procédures (Les 30 procédures), les rapports antérieurs, etc, nécessaires à l'audit.

3.8.2- Réalisation des Audits :

Conduire les audits conformément au programme établi en utilisant des techniques appropriées d'entrevues, d'observations et d'analyses de documents, et suivant la checklist ISO 28000-2007.

Sous- section Check List	Libellé	Affectation
4.1	Overall Security Management System	Mme B.H
4.2	Policy	Mme K.Y
4.3.1	Security Risk Assessment	Mme B.H
4.3.1 (Cont)	Security Risk Assessment (continued)	Mme B.H
4.3.2	Legal, Statutory and Other Security Regulatory Requirements	Mr S.H
4.3.3	Objectives	Mr C.M
4.3.4	Targets	Mr C.M
4.3.5	Programmes	Mr C.M
4.4.1	Structure, Authority and Responsibility	Mr B.N
4.4.1 (cont)	Structure, Authority and Responsibility (continued)	Mr B.N
4.4.2	Competence, Training and Awareness	Mr B.N
4.4.3	Communication	Mme K.Y
4.4.4	Documentation	Mme K.Y
4.4.5	Document and Data Control	Mr C.M
4.4.6	Operational Control	Mr Z.M
4.4.7	Emergency Preparedness, Response and Security Recovery	Naoufel
4.5.1	Security Performance Measurement and Monitoring	Mr B.S
4.5.1 (cont)	Security Performance Measurement and Monitoring (continued)	Mr B.S
4.5.2	System Evaluation	Mr S.H
4.5.3	Security-related Failures, Incidents, Non-conformances and Corrective and Preventive Actions	Mr Z.M
4.5.3 (cont)	Security-related Failures, Incidents, Non-conformances and Corrective and Preventive Actions (continued)	Mr Z.M
4.5.4	Control of Records	Mr B.S
4.5.5	Audit	Mme B.H
4.5.5 (cont)	Audit	Mme B.H
4.6	Management Review and Continual Improvement	Mr S.H

Tableau N°05 : La Répartition des sections de travail (Source : élaboré par nos soins)

4- Résultats de la mission :

4.1- Collecte des résultats :

Revient à rassembler tous les résultats de l'audit, y compris les constatations, les conclusions et les recommandations.

4.2- Identification des écarts :

Implique l'analyse des résultats pour identifier les écarts entre les pratiques actuelles et la norme (ISO28000), puis classez les écarts en fonction de leur gravité et de leur impact sur l'organisation.

Chapitre 03 : Cas pratique (Cas : de la filiale Algérienne D)

Risque N°	Discription de l'évenement	Criticité
1	Bien que le manuel des procédures soit en place, il est observé que certaines procédures ne sont appliquées que partiellement	Elevé
2	La documentation concernant la surveillance des actions pour assurer l'efficacité et la rapidité de leur mise en œuvre de l'évaluation de la sécurité (tableaux de Board KPI) n'existe pas.	Elevé
3	Les objectifs sont bien définis, mais il n'y a pas de colonne pour la prioritisation. Selon le Directeur de la Sureté, les trois niveaux inclus dans le plan décrivent la priorité (descendante de la plus élevée à la plus basse).	Moyen
4	Les objectifs doivent être créées en fonction des problèmes spécifiques et des moyens d'amélioration. Il n'y a pas d'identification claire des problèmes pour motiver les objectifs.	Elevé
5	Il n'y a pas de suggestions de la part des employés et des parties intéressées en vue d'améliorer le système de la sureté. Le formulaire de commentaires existe , il a été envoyé aux interessés mais aucun retour n'est enregistré.	Moyen
6	La distruction des documents obsolètes est formalisée , mais il n'y a pas d'évidences.(Aucun document de distruction n'est trouvé)	Moyen
7	"Il existe plusieurs procédures opérationnelles pour prendre en compte les risques de sécurité, en particulier : 1) Procédure opérationnelle de sécurité SMP 18 ; - Procédure de contrôle d'accès SMP 18.1 ; - Procédure CCTV SMP 18.2 ; (Cependant, ces deux procédures ne sont pas opérationnelles) 2) De plus, les procédures suivantes manquent toujours : - Interface avec le navire - Manipulation de la cargaison - Procédure pour les zones restreintes."	Extreme
8	SMP22-R01 Programme de simulations et d'exercices de sécurité : La planification détaillée des simulations et exercices n'est pas exhaustive, les dates et heures ne sont pas bien détaillées.	Moyen
9	Le processus d'analyse des dossiers est effectué chaque mi-année, le fichier détaille toutes les analyses de sécurité, incidents, formations, actions correctives, etc. À développer davantage.	Faible

Tableau n°06 : Le Registre des risques « Risque Register » et/ou les non-conformités identifiées, (Source : élaboré par nos soins)

4.3- Évaluation des risques :

Signifie l'évaluation des risques associés à chaque non-conformité identifiée. Cela peut inclure l'évaluation de l'impact potentiel sur les opérations.

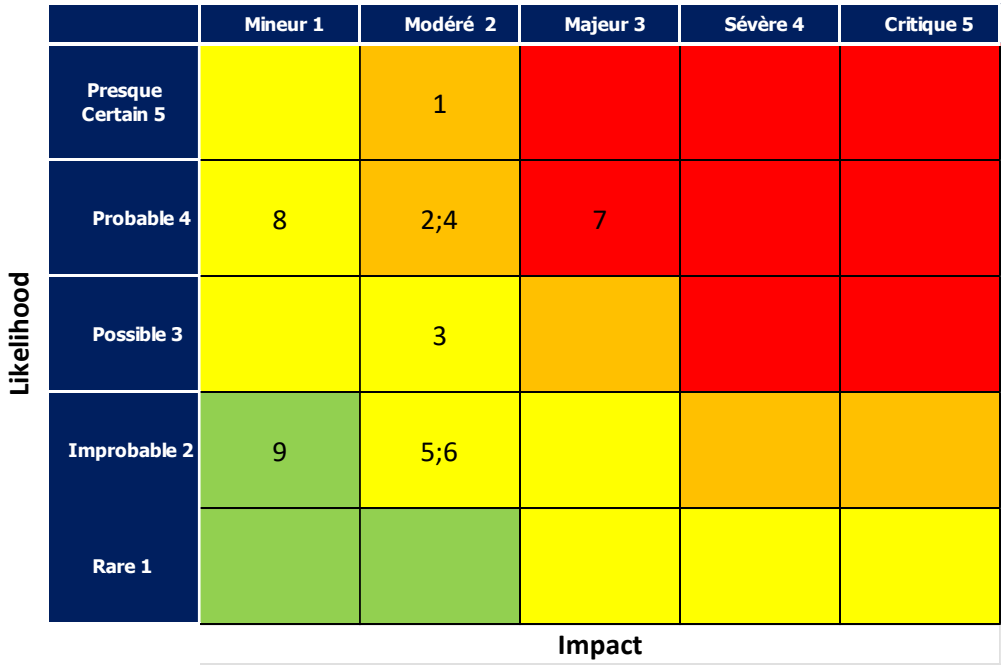


Figure n°09 : La cartographie des risques (Source : élaboré par nos soins)

- ✓ Les risques N°1,2,4 et 8 : Nécessitent un traitement pour réduire le risque et améliorer le processus.
- ✓ Le risque N°7 : Requière une prise en charge immédiate et prioritaire, il s'agit d'une zone de défi. Le risque étant majeur.
- ✓ Les risques N°3,5,6 et 9 : Nécessitent une surveillance régulière afin d'aider le département de sureté à mettre en place une solution.

4.4- Priorisation des actions correctives :

A pour résultat de classer les risques en fonction de leur priorité. En se concentrant sur les écarts (les non-conformités) les plus critiques ou ceux qui présentent le plus grand risque pour l'entreprise.

Chapitre 03 : Cas pratique (Cas : de la filiale Algérienne D)

Risque N°	Discription de l'évenement	Criticité	Prioritisation (De 1 jusqu'à 9)
1	Bien que le manuel des procédures soit en place, il est observé que certaines procédures ne sont appliquées que partiellement	**Elevé**	2
2	La documentation concernant la surveillance des actions pour assurer l'efficacité et la rapidité de leur mise en œuvre de l'évaluation de la sécurité (tableaux de Board KPI) n'existe pas.	**Elevé**	4
3	Les objectifs sont bien définis, mais il n'y a pas de colonne pour la prioritisation. Selon le Directeur de la Sureté, les trois niveaux inclus dans le plan décrivent la priorité (descendante de la plus élevée à la plus basse).	**Moyen**	5
4	Les objectifs doivent être créées en fonction des problèmes spécifiques et des moyens d'amélioration. Il n'y a pas d'identification claire des problèmes pour motiver les objectifs.	**Elevé**	3
5	Il n'y a pas de suggestions de la part des employés et des parties intéressées en vue d'améliorer le système de la sureté. Le formulaire de commentaires existe , il a été envoyé aux interessés mais aucun retour n'est enregistré.	**Moyen**	6
6	La distruction des documents obsolètes est formalisée , mais il n'y a pas d'évidences.(Aucun document de distruction n'est trouvé)	**Moyen**	8
7	"Il existe plusieurs procédures opérationnelles pour prendre en compte les risques de sécurité, en particulier : 1) Procédure opérationnelle de sécurité SMP 18 ; - Procédure de contrôle d'accès SMP 18.1 ; - Procédure CCTV SMP 18.2 ; (Cependant, ces deux procédures ne sont pas opérationnelles) 2) De plus, les procédures suivantes manquent toujours : - Interface avec le navire - Manipulation de la cargaison - Procédure pour les zones restreintes."	**Extreme**	1
8	SMP22-R01 Programme de simulations et d'exercices de sécurité : La planification détaillée des simulations et exercices n'est pas exhaustive, les dates et heures ne sont pas bien détaillées.	**Moyen**	7
9	Le processus d'analyse des dossiers est effectué chaque mi-année, le fichier détaille toutes les analyses de sécurité, incidents, formations, actions correctives, etc. À développer davantage.	**Faible**	9

Tableau N°07 : Classement des risques par ordre de priorité, du plus critique au moins critique. (Source : élaboré par nos soins)

5- Développement d'un plan d'action :

Cette étape se caractérise par la mise en place d'un plan d'action détaillé et/ou recommandations pour remédier à chaque écart. Ce plan inclut des étapes spécifiques, et des responsabilités claires pour atténuer les risques constatés.

Chapitre 03 : Cas pratique (Cas : de la filiale Algérienne D)

Risque N°	Discription de l'évenement	Criticité	Prioritisation	Recommandations
1	Bien que le manuel des procédures soit en place, il est observé que certaines procédures ne sont appliquées que partiellement	Elevé	2	Il est crucial de mettre en œuvre des mesures correctives pour garantir une conformité totale avec l'ensemble des procédures définies, assurant ainsi une exécution uniforme et efficace des processus au sein de l'organisation.
2	La documentation concernant la surveillance des actions pour assurer l'efficacité et la rapidité de leur mise en œuvre de l'évaluation de la sécurité (tableaux de Board KPI) n'existe pas.	Elevé	4	Mise en place de tableaux de board pour les indicateurs clés permettant de suivre de manière transparente les données de surveillance, et afin d'optimiser la gestion et l'amélioration continues des processus de sécurité de l'organisation.
3	Les objectifs sont bien définis, mais il n'y a pas de colonne pour la prioritisation. Selon le Directeur de la Sureté, les trois niveaux inclus dans le plan décrivent la priorité (descendante de la plus élevée à la plus basse).	Moyen	5	Nous suggérons l'intégration d'une colonne de prioritisation dans la documentation des objectifs. Selon les indications du Directeur de la Sûreté, les trois niveaux actuels inclus dans le plan peuvent être utilisés pour décrire la priorité de manière descendante, de la plus élevée à la plus basse. L'ajout de cette colonne permettra une identification plus claire des priorités, facilitant ainsi la mise en œuvre efficace des objectifs définis et renforçant l'alignement stratégique au sein de l'organisation."
4	Les objectifs doivent être créées en fonction des problèmes spécifiques et des moyens d'amélioration. Il n'y a pas d'identification claire des problèmes pour motiver les objectifs.	Elevé	3	Nous recommandons d'améliorer le processus de définition des objectifs en les alignant de manière plus spécifique sur les problèmes identifiés et les moyens d'amélioration. Actuellement. Nous suggérons de mettre en place un mécanisme structuré d'identification des problèmes, peut-être à travers des évaluations régulières, des retours d'expérience ou des analyses approfondies. Cela permettra de formuler des objectifs plus pertinents, directement liés aux défis spécifiques de l'organisation, favorisant ainsi une amélioration ciblée et efficace.
5	Il n'y a pas de suggestions de la part des employés et des parties intéressées en vue d'améliorer le système de la sureté. Le formulaire de commentaires existe , il a été envoyé aux interessés mais aucun retour n'est enregistré.	Moyen	6	Nous recommandons de promouvoir activement la participation des employés et des parties intéressées dans l'amélioration continue du système de sûreté. Bien que le formulaire de commentaires soit disponible et ait été envoyé aux parties concernées, le manque de retours enregistrés suggère la nécessité de sensibiliser davantage et d'encourager la contribution. Il serait bénéfique d'instaurer des initiatives de communication régulières, de souligner l'importance des retours d'expérience et de fournir des incitations pour stimuler la participation. Cela contribuera à une culture de sécurité collaborative, favorisant une identification proactive des opportunités d'amélioration au sein de l'organisation.
6	La distruction des documents obsolètes est formalisée , mais il n'y a pas d'évidences.(Aucun document de distruction n'est trouvé)	Moyen	8	Nous recommandons de renforcer le processus de destruction des documents obsolètes en fournissant des preuves tangibles de chaque opération de destruction. Bien que la formalisation du processus soit en place, l'absence d'évidence, telle que la documentation de destruction, soulève des préoccupations en matière de conformité et de suivi. Il est conseillé de mettre en œuvre un système de suivi rigoureux qui documente de manière systématique chaque opération de destruction, y compris les détails pertinents tels que la date, la nature des documents détruits et le responsable de l'opération. Cela garantira une traçabilité adéquate et renforcera la transparence du processus de gestion documentaire.
7	"Il existe plusieurs procédures opérationnelles pour prendre en compte les risques de sécurité, en particulier : 1) Procédure opérationnelle de sécurité SMP 18 ; - Procédure de contrôle d'accès SMP 18.1 ; - Procédure CCTV SMP 18.2 ; (Cependant, ces deux procédures ne sont pas opérationnelles) 2) De plus, les procédures suivantes manquent toujours : - Interface avec le navire - Manipulation de la cargaison - Procédure pour les zones restreintes."	Extreme	1	Nous recommandons d'élaborer et de documenter les procédures manquantes pour assurer une gestion complète des opérations.. Il est crucial d'élaborer des directives détaillées pour ces domaines afin d'assurer une exécution efficace et sécurisée des opérations. Nous suggérons d'impliquer les parties concernées dans le processus d'élaboration des procédures afin de garantir une compréhension approfondie et une conformité opérationnelle.
8	SMP22-R01 Programme de simulations et d'exercices de sécurité : La planification détaillée des simulations et exercices n'est pas exhaustive, les dates et heures ne sont pas bien détaillées.	Moyen	7	Nous recommandons d'améliorer la planification détaillée des simulations et exercices en rendant le processus plus exhaustif. Actuellement, les dates et heures ne sont pas suffisamment détaillées. Il est conseillé d'élaborer un calendrier plus précis, incluant des détails spécifiques sur le timing, et les participants prévus pour chaque simulation ou exercice. Une planification plus détaillée permettra une préparation adéquate, une exécution plus fluide et une évaluation approfondie des performances, contribuant ainsi à renforcer la robustesse du programme de simulation et d'exercices."
9	Le processus d'analyse des dossiers est effectué chaque mi-année, le fichier détaille toutes les analyses de sécurité, incidents, formations, actions correctives, etc. À développer davantage.	Faible	9	Nous recommandons de renforcer et d'approfondir le processus d'analyse des dossiers effectué chaque mi-année. Bien que le fichier actuel détaille divers éléments tels que les analyses de sécurité. Nous suggérons d'inclure plus d' indicateurs de performance clés (KPI) pertinents, d'analyser les tendances au fil du temps, et d'établir des liens plus étroits entre les différentes composantes des analyses. Ceci permettra une évaluation plus approfondie des performances, une identification proactive des domaines d'amélioration, et une prise de décision plus informée pour renforcer globalement la sûreté et la sécurité de l'organisation.

Tableau N°08 : Les recommandations détaillées à mettre en place pour chaque risque. (Source : élaboré par nos soins)

6- Les Résultats :

Consiste à enregistrer toutes les non-conformités, les observations, constatations et recommandations découlant de l'audit.

Formalisation de la synthèse d'audit (Rapport d'audit).

7- Clôture de l'audit :

Nous avons procédé à la clôture de la session d'audit en organisant une réunion avec le Manager de la sureté et son équipe, afin de communiquer et partager les résultats de l'audit, les écarts identifiés et le plan d'action.

Nous avons par la suite suivi l'application des recommandations afin d'éliminer les risques existants avant le début de l'audit de Certification.

Donc cette phase, constitue une évaluation préliminaire visant à identifier les lacunes par rapport aux exigences de la norme ISO 28000.

Section 03 :

L'Audit Externe (Certification)

La certification ISO (Internationale Organisation for Standardisation) est un processus par lequel la société va démontrer sa conformité à la norme ISO 28000. Les étapes générales et typiques suivies pour obtenir la certification de la norme, sont les suivantes :

1- **Évaluation initiale :** Avant de s'engager dans le processus de certification, la société a effectué une évaluation initiale pour identifier les lacunes par rapport aux exigences de la norme ISO susvisée. Cette évaluation a été réalisé par l'équipe d'audit Interne (voir section 2).

2- **Formation et sensibilisation :** Les employés et la direction de Sureté ont été formés aux exigences de la norme ISO 28000. De Plus, Une sensibilisation à la culture de la qualité et aux objectifs de la certification, a été accordé en interne pour l'ensemble des employés de la société, et pour laquelle nous avons mis en place les moyens nécessaires pour l'accomplir et suivre l'avancement de l'opération de près.

3- **Pré-audit (facultatif) :** Nous avons choisi de réaliser un pré-audit avec l'organisme international de certification indépendant « Le cabinet L » pour évaluer notre préparation avant l'audit de certification officiel.

Ci-dessous les résultats du pré-Audit :

3.1- Evaluation :

Management : La politique est claire, connue et communiquée. La direction est impliquée dans l'amélioration continue, elle donne les moyens et participe aux comités utiles au bon fonctionnement de la sureté.

Examen de la documentation du système, de la structure organisationnelle, des responsabilités, des autorités, des compétences et de la formation du personnel : Les autorités et responsabilités des équipes sureté sont claire au travers de leur fiche de poste. Le reste des effectifs est formé et sensibilisé à la sureté par un formateur interne ; les émargements sur les fiches de présence démontrent ce suivi et la couverture des effectifs de façon globale. La documentation sureté abordée et vue ce jour est clairement structurée pour prendre en compte et couvrir les exigences documentaires de l'ISO 28000/2007 et aussi celles du « Groupe D ». On y retrouve la politique sureté, le manuel, les procédures et les formulaires. La documentation électronique et papier est bien gérée. Tous les documents internes sont tous clairement classifiés suivant leur niveau de confidentialité et clairement libellé sur le document lui-même. Les documents d'origine externe comme l'ISPS, ISO28000 et standards sont disponibles et sous contrôle du fichier Excel correspondant La conformité au référentiel ISO 28000/2007 est démontrée sur les points de ce jour.

3.2- Points d'améliorations :

Ci-dessous les points d'améliorations détectés par le « Cabinet L » :

- ✓ Les cibles ne sont pas clairement documentées sur le tableau de suivi quotidien des KPI même si elles sont très claires pour les interviewés.
- ✓ A l'issue des formations/sensibilisations sureté, il pourrait être envisagé la réalisation d'un petit quizz pour mesurer l'efficacité de la formation et sa compréhension.
- ✓ La procédure SMP18.1 v1.0 03/22 Contrôle accès ne traite pas clairement les modalités d'accès des chauffeurs et des camions/conteneurs (problème de formalisme ; la pratique est très claire et opérationnelle).
- ✓ Sur le tableau de registre des incidents, la colonne commentaires n'est pas rempli pour démontrer l'action réalisée et son efficacité.
- ✓ Si la revue de direction a été réalisée suivant un agenda complet et en cohérence avec l'ISO 28000/2007, le compte-rendu ne met pas en valeur les points abordés (Ex : point 15 de l'agenda sur les Incidents et NC : sans commentaire).
- ✓ La révision de l'ISO 28000/2022 de mars 2022 n'a pas été identifiée par la structure.
- ✓ Il est fortement recommandé que l'équipement de sécurité aux portes comprenne :

  - détecteurs de métaux (Déjà en cours d'achat),
  - Boutons de feux de signalisation,

- ✓ Une formation en langage corporel axée sur la sécurité est recommandée pour le personnel de gardiennage.
- ✓ Il a été recommandé que les visites aux postes de sécurité par le superviseur de la sécurité soient consignées dans le registre quotidien (l'enregistrement peut inclure le statut, le rendement, l'heure et le nom du poste, suggérés pour être de couleur différente).
- ✓ Pour les exercices qui ne se déroulent pas à la période planifiée, envisager d'inclure un dossier indiquant la date réelle de l'exercice et la raison du retard ou de l'annulation.
- ✓ Les recommandations ou les mesures fondées sur l'évaluation des résultats des exercices peuvent également (le cas échéant) inclure un « examen et une mise à jour » des contrôles établis dans le registre d'évaluation des risques.

4- Audit de certification : L'organisme de certification international « Le cabinet L » a effectué l'audit de certification pour évaluer si l'entreprise respecte les exigences de la norme. Cela a inclut des entretiens, des examens de documents (Y compris le rapport d'audit interne) et des observations sur site en présence du Manager de la sureté, Risk and Compliance Manager et des collaborateurs du département de la sureté.

5- Rapport d'Audit Final : L'organisme de certification « Le cabinet L » a envoyé un rapport d'audit détaillé qui identifie les forces du système de gestion de la sureté par rapport à la norme ISO. Ainsi, les faiblesses soit deux non-conformités soulevées.

Ci-dessous le détail de l'opinion finale « Rapport du Cabinet L » :

5.1- Evaluation :

- ➢ Documentation

- ✓ La documentation sureté abordée et vue ce jour est clairement structurée pour prendre en compte et couvrir les exigences documentaires de l'ISO 28000/2007. On y retrouve la politique sureté, le manuel, les procédures et les forms.
- ✓ La documentation électronique et papier est bien gérée.
- ✓ Tous les documents internes sont tous clairement classifiés suivant leur niveau de confidentialité et clairement libellé sur le document lui-même.
- ✓ Les documents d'origine externe comme l'ISPS, et ISO28000, standards sont disponibles et sous contrôle du fichier Excel correspondant.

- ✓ La conformité au référentiel ISO 28000/2007 est démontrée sur les points de ce jour avec la correction de la procédure SMP 18 pour prendre en compte la remarque sur les camions lors de la phase 1.

➢ Top Management (security policies, objectives, achievements, security initiatives and improvement plans)

- ✓ La politique est claire, connue et communiquée.
- ✓ La direction est impliquée dans l'amélioration continue ; elle donne les moyens et participe aux comités utiles au bon fonctionnement de la sureté.
- ✓ Les revues de direction semestrielles ont été réalisées en 06 & 11/22 : elles sont globalement complètes par rapport aux agendas et exigences de l'ISO 28000.
- ✓ Les autorités et responsabilités des équipes sureté sont claire au travers de leur fiche de poste. Le reste des effectifs est formé et sensibilisé à la sureté.

➢ Evaluation des risques sureté

- ✓ L'évaluation est conforme en termes d'assets et d'action de protection.
- ✓ Des actions sont en cours pour diminuer les intrusions sur le site, le port des badges.
- ✓ Le suivi et le traitement des incidents est globalement démontré sur les exemples vus avec maintenant une meilleure formalisation de l'action et de son efficacité.
- ✓ Le suivi des NC et ACP est bien documenté et démontré au travers des points audités ; à ce stade la plupart des NC émises et des pistes d'améliorations traitées sont issues de l'audit interne de 09/22.
- ✓ L'analyse du registre des incidents pourrait permettre de continuer à alimenter ce registre et l'amélioration continue.

➢ Audit Interne

- ✓ L'audit interne du SMS a été réalisé de façon très professionnelle et très bien documenté par une équipe de 6 auditeurs qualifiés en 09/22 ; les écarts ont fait et font encore pour certains l'objet d'un suivi et d'un traitement au travers des fiches et du registre des NC.
- ✓ La phase 2 permet de constater des progrès et des améliorations et des actions à plus long terme.

- Les obligations Légales

- ✓ La veille réglementaire est globalement bien mise en oeuvre et suivie.
- ✓ Une aide externe est en cours de recherche pour aider l'équipe dans ce vaste et fastidieux travail.

- Situations urgence et exercices

- ✓ Les situations d'urgence sont bien identifiées ainsi que les consignes à appliquer.
- ✓ Un planning annuel est établi et suivi.
- ✓ Les exercices pour 2022 ont été réalisés et ont fait l'objet de compte-rendus et de retours d'expérience et d'actions si nécessaire.

- Ressources Humaines

- ✓ La fonction RH prend bien en compte la notion de sureté pour en informer et associer le personnel
- ✓ Les formations indispensables au règlement ISPS sont réalisées et démontrées pour les équipes de sureté ainsi que des sensibilisations pour les autres.
- ✓ Les nouveaux sont accueillis et bien informés en termes de sécurité et de sureté ainsi que les intervenants externes.
- ✓ Plusieurs pistes de progrès sont toutefois identifiées.

- Commercial

- ✓ Les activités commerciales démontrent l'importance et la demande des clients en termes de sureté.
- ✓ Le suivi est démontré.

- Procurement

- ✓ La sélection et le choix des prestataires externes est clairement établi et documenté. Les commandes et les approvisionnements sont bien réalisés.
- ✓

- IT

- ✓ La sureté au niveau informatique est très bien prise en compte au travers des points précédemment listés et gérés.

5.2- Conclusion :

- Points d'améliorations

- ✓ Alors que l'intrusion est un des plus forts risques évalués, le planning des exercices ne le prévoit pas.
- ✓ Les actions doivent continuer pour diminuer les intrusions et le respect des consignes des chauffeurs.
- ✓ Les fiches de postes actuelles ne document pas clairement les compétences et habilitations nécessaires : l'utilisation des formulaires permettrait d'améliorer ce point.(action en cours).
- ✓ A l'issue des formations/sensibilisations sureté, il pourrait être envisagé la réalisation d'un petit quizz pour mesurer l'efficacité de la formation et sa compréhension (action en cours).
- ✓ Il n'existe pas de suivi permettant de démontrer que tout le personnel a suivi la formation/sensibilisation à la sureté et à l'ISO28000 ; ainsi que les actions à mener pour ceux n'ayant pas reçu la sensibilisation.
- ✓ Actuellement, il n'y a pas de caméras de vidéosurveillance dédiées sur le quai. Une caméra de vidéosurveillance installée sur le bâtiment administratif fournit une vue distante, démontrée lors de la visite de la salle de contrôle.
- ✓ Des plans pour installer plus de caméras de vidéosurveillance côté quai, soutenus par le budget, ont été mis en évidence lors de réunions ultérieures avec la gestion de la sécurité et les finances.
- ✓ Documentation sur ISPS à compléter pour démontrer la conformité de la « filiale Algérienne D ».
- ✓ Induction de sécurité pour les employés restants du fournisseur de Nettoyage encore à compléter.
- ✓ Salle de contrôle : envisager de conserver les déclarations de confidentialité signées pour tous les opérateurs.
- ✓ Le plan de maintenance préventive pourrait inclure le niveau de priorité et la raison du retard ou du report documenté.
- ✓ Le formulaire d'évaluation du fournisseur pourrait inclure un critère d'acceptation basé sur la note finale qui montre clairement un résultat satisfaisant ou non satisfaisant.

6- Actions Correctives : La société a mis en place des actions correctives pour remédier aux non-conformités soulevées.

L'organisme de certification a parvenu un délai de correction des non-conformités.

7- **Certification :** « Le cabinet L » a élaboré une seconde vérification afin de s'assurer si les non-conformités identifiées ont été corrigées. Après vérification, l'organisme de certification a délivré le certificat de conformité à l'entreprise en Décembre 2022.

8- **Surveillance continue et audits de suivi :** Nous devons maintenir notre système de gestion de la qualité de la sureté conformément à la norme ISO 28000 et être prêts à des audits de suivi périodiques de la part de l'organisme de certification.

Conclusion du chapitre :

Dans ce Chapitre, notre objectif principal était de présenter la pratique de l'Audit Interne Outil du Risk Management en mettant en évidence le rôle important de l'Audit Interne dans la gestion des risques liés à la sureté.

Nous avons commencé par présenter le lieu de stage où nous avons réalisé notre étude de cas, qui était l'entreprise « La filiale Algérienne D », détaillant les différents services, l'organigramme ainsi que les missions de chaque département.

Dans la deuxième section, nous avons procédé à l'Audit Interne de la fonction Sureté afin de déterminer l'efficacité des processus de sureté existants, de mettre en évidence les lacunes éventuelles et de fournir des recommandations pour améliorer la gestion de l'entreprise face aux risques.

Dans la troisième section, nous avons examiné de près les étapes de Certification ISO 28000 de la chaine d'approvisionnement élaborées par l'organisme de Certification « Cabinet L » dont les deux principales étapes : pré-audit et Audit de Certification. Nous avons mis en évidence les deux volets de cette pratique.

L'objectif de ce chapitre est de présenter une vue d'ensemble exhaustive de la mise en œuvre de la Certification ISO 28000 qui apporte une approche systématique et standardisée à la gestion de la sécurité de la chaîne d'approvisionnement, offrant une gamme d'avantages à savoir :

- **Amélioration de l'Image de Marque :** Afficher une certification ISO 28000 démontre l'engagement envers la sécurité de la chaîne d'approvisionnement et peut renforcer la confiance des clients, des partenaires commerciaux et des parties prenantes.

- **Efficacité Opérationnelle :** La mise en œuvre de pratiques de sécurité efficaces peut améliorer l'efficacité opérationnelle en réduisant les perturbations liées à des incidents de sécurité.

- **Avantages Concurrentiels :** La certification ISO 28000 peut être un facteur différenciant sur le marché, démontrant un engagement envers la sécurité et la fiabilité de la chaîne d'approvisionnement.

- **Réduction des Coûts :** En minimisant les risques de perturbations, de vols et d'autres incidents liés à la sécurité, une organisation peut potentiellement réduire les coûts associés aux interruptions de la chaîne d'approvisionnement.

Nous devons promouvoir une culture organisationnelle qui valorise l'Audit Interne et le Risk Management en tant qu'outil d'amélioration continue et/ou de qualité.

CONCLUSION

Conclusion

En conclusion, l'environnement économique d'aujourd'hui est devenu plus complexe et plus sophistiqué, ce qui rend les entreprises plus exposées aux divers risques. Notre étude approfondie sur le rôle de l'audit interne en tant qu'outil du Risk management a mis en lumière l'importance cruciale de cette fonction dans la gestion des risques, en mettant l'accent sur une entreprise de taille et activité importante dans le contexte Algérien.

L'audit interne, en tant que processus systématique d'évaluation et d'assurance, offre une perspective holistique permettant d'identifier, évaluer et atténuer les risques opérationnels, financiers et stratégiques auxquels une entreprise est exposée.

Nous avons souligné l'évolution du contexte économique, réglementaire et technologique, qui a considérablement accru la complexité des risques auxquels les entreprises sont confrontées. Dans ce contexte, l'audit interne émerge comme un outil essentiel, offrant une approche proactive pour anticiper et gérer les risques, plutôt que de simplement les réagir après qu'ils se sont matérialisés.

Notre analyse a également mis en évidence le lien étroit entre l'audit interne et le Risk management, soulignant la nécessité d'une collaboration étroite entre ces deux fonctions au sein de l'entreprise. L'intégration efficace de l'audit interne dans le processus global de gestion des risques garantit une meilleure compréhension des enjeux, une identification plus précise des vulnérabilités et une mise en place de mécanismes de contrôle plus robustes.

En outre, l'Audit Interne et le Risk Management ont été examinée en détail dans la théorie et démontrée dans la pratique, cela inclut l'examen des conditions de mise en œuvre de meilleures pratiques en matière d'audit interne, soulignant l'importance de l'indépendance, de la compétence, de la transparence et de la communication dans la réalisation d'audits efficaces. Ces principes, combinés au principe de Risk Management, renforcent la capacité de l'audit interne à fournir des recommandations pertinentes et opportunes pour la gestion des risques.

Examen des hypothèses :

Hypothèse 1 : Cette hypothèse suggère que la mise en place des technologies de surveillance avancées, telles que la vidéosurveillance intelligente, contribuent à une détection plus rapide et plus précise des menaces dans la chaîne d'approvisionnement de la sûreté.

En théorie, une surveillance avancée peut détecter des incidents de manière précoce, ce qui pourrait contribuer à une intervention rapide et à la prévention de situations dangereuses. Cependant, l'implémentation de technologies de surveillance avancées

soulève des préoccupations en matière de vie privée. Il est important de trouver un équilibre entre la sécurité et le respect des droits individuels. La mise en place de technologies de surveillance avancées peut également impliquer des coûts importants en termes d'infrastructure, de maintenance et de formation du personnel.

En résumé, bien que la vidéosurveillance intelligente puisse potentiellement contribuer à une détection plus rapide et plus précise des menaces dans la chaîne d'approvisionnement de la sûreté, son efficacité dépend de divers facteurs et de la manière dont elle est mise en œuvre. Une approche équilibrée, prenant en compte la vie privée, la précision, et les coûts, est essentielle pour maximiser les avantages de ces technologies tout en minimisant les inconvénients.

Hypothèse 2 : L'amélioration des programmes de formation du personnel sur la sensibilisation aux menaces et aux protocoles de sécurité conduit à une meilleure réactivité face aux incidents.

En effet, L'amélioration des programmes de formation du personnel en matière de sensibilisation aux menaces et de protocoles de sécurité peut considérablement contribuer à renforcer la réactivité face aux incidents de sécurité.

En étant bien formés, les employés sont mieux préparés à réagir rapidement et efficacement en cas d'incident de sécurité. Cependant la formation seule ne suffit pas, la mise en œuvre de mesures d'atténuation d'urgence et la collaboration pour contenir et résoudre rapidement les problèmes.

Hypothèse 3 : Cette hypothèse suggère que les entreprises qui s'alignent rigoureusement sur les normes et réglementations de sûreté réussissent mieux à instaurer des systèmes performants de gestion des menaces et des incidents dans leur chaîne d'approvisionnement.

Ce qui est totalement vrai, car les normes et réglementations de sûreté sont généralement conçues pour garantir un niveau minimum de sécurité dans divers secteurs. En suivant ces normes, les entreprises peuvent mettre en place des pratiques qui réduisent les risques liés à la sécurité des opérations et sont souvent mieux préparées à faire face aux menaces et aux incidents.

Bien que la conformité puisse entraîner des coûts initiaux, elle peut également contribuer à réduire les coûts à long terme liés aux incidents de sécurité.

Conclusion

Résultats et Recommandations :

L'audit interne et la Gestion des Risques sont deux fonctions essentielles au sein d'une organisation, et leur lien est crucial pour assurer une gouvernance efficace. La couverture des risques se fait à travers le Contrôle Interne de l'entreprise mais l'assurance ne peut se faire qu'à travers l'Audit.

L'audit interne fournit une assurance indépendante sur l'efficacité des processus de gestion des risques. Cette assurance est précieuse pour les parties prenantes internes et externes, y compris les actionnaires, les dirigeants, les régulateurs et les investisseurs. L'audit interne s'assure que les objectifs de l'organisation sont alignés avec sa tolérance au risque. Cela garantit que la gestion des risques est en accord avec la stratégie globale de l'entreprise. L'audit interne peut ainsi jouer un rôle dans le processus d'amélioration continue en recommandant des ajustements dans les politiques, les procédures et les pratiques de gestion des risques.

En effet, la capacité à comprendre le lien entre l'Audit interne et le Risk Management est bénéfique aux entreprises pour répondre efficacement à Gestion des Risques et optimiser les couts.

A ce jour la réglementation Algérienne peut évoluer et réglementer l'activité du Risk Management pour toutes les entreprises et leurs activités.

Les limites :

L'étude de l'audit interne outil du Risk Management est un domaine vaste et complexe. Malgré les limitations et les contraintes de temps auxquelles nous avons été confrontés, nous avons entrepris cette étude. Cependant, il est important de mentionner certaines limites :

La théorie de l'Audit Interne outil du Risk Management est souvent difficile à trouver car les ouvrages qui en traitent sont limités, et les études Algériennes sur ce sujet sont rare.

Les réglementations en matière de la gestion des risques en Algérie, prévoit de souscrire à des assurances spécifiques liées aux risques liés à leurs activités, loi sur la santé et sécurité au travail, les règlements de la Banque d'Algérie en ce qui concerne le contrôle interne des institutions financières (loi 11-08) et essentiellement les banques devront impérativement dispose un système de surveillance de ses propres risques.

Conclusion

Les perspectives de l'étude :

Nous reconnaissons que notre travail n'est pas parfait, car le sujet du Risk Management et l'Audit Interne est multidimensionnel et peut être abordé de différentes manières, telles que l'intégration stratégique « la contribution du RM et AI dans l'atteinte des objectifs » , l'efficacité opérationnelle « la contribution du RM et l'AI pour améliorer la résilience opérationnelle », la conformité réglementaire (Standards International ISO) « Garantir la conformité aux réglementations en vigueur et minimiser les risques liés aux non-conformités ».

Cependant, ce qui nous a particulièrement intéressé est une question que nous avons posée après une étude documentaire de plus de 4 mois. Nous nous sommes penchés sur la problématique de trouver un point optimal qui satisfait à la fois le gouvernement et les entreprises. En effet, bien que l'Audit et le Risk Management permettent de réduire et minimiser les risques liés aux non-conformités, il n'existe pas des textes réglementaires qui cadre ce contexte en Algérie, ce sujet a suscité notre intérêt et il représente une autre facette importante ainsi qu'un autre aspect de Continuité d'activité. Nous recommandons vivement aux générations futures de s'intéresser à ces sujets.

Bibliographie

Les ouvrages

1. Cadre de référence internationale (IIA) – cadre de référence internationale des pratiques professionnelles -Edition 2017.
2. Pratique de l'Audit. « Editions BERTI », Auteur : Mokhtar BELAIBOUD, docteur d'Etat en sciences de gestion, Expert-comptable et commissaire aux comptes.
3. "Contrôle Interne - Des fondamentaux aux bonnes pratiques" par Anne Germain et Jean-Pierre Hugot.
4. Théorie et pratique de l'Audit Interne, Jacques Renard éditions EYROLLES
5. "Business Process Reengineering : Breakpoint Strategies for Market Dominance" par Michael Hammer et James A. Champy.
6. "The Phoenix Project : A Novel About IT, DevOps, and Helping Your Business Win" par Gene Kim, Kevin Behr, et George Spafford.
7. Audit et Contrôle Interne « Benoit PIGé », éditions EMS « Management et société » ;
8. Principles of Auditing: An International Perspective par Rick Stephan Hayes, Arnold Schilder, Roger Dassen, Philip Wallage McGraw-Hill, 1999
9. Audit Interne, Elisabeth Bertin, éditions EYROLLES ;
10. Institute of Internal Auditors (IIA). (2021). "International Standards for the Professional Practice of Internal Auditing."
11. « Théorie et pratique de l'Audit Interne », Jacques Renard,9éme édition EYROLLES.
12. « Théorie et pratique de l'Audit Interne », Jacques Renard,9éme édition EYROLLES.
13. The Invisible Hand : How an Insurer Thinks about Risk" par Kenneth S. Abraham.
14. Risk Management and Insurance" par Scott E. Harrington et Gregory R. Niehaus
15. Enterprise Risk Management : From Incentives to Controls" par James Lam.
16. La Norme ISO 31000 version 2018.
17. "Risk Management : Concepts and Guidance",fifth edition 2015, par Carl L. Pritchard.Edition.
18. Risk Management : Concepts and Guidance",fifth edition 2015, par Carl L. Pritchard.Edition.
19. Risk Management : Concepts and Guidance",fifth edition 2015, par Carl L. Pritchard.Edition.
20. "The Essentials of Risk Management" Second edition2014, par Michel Crouhy, Dan Galai, Robert Mark.
21. Lean Thinking : bannissez le gaspillage et créez de la richesse dans votre entreprise,Janvier 1996,Journal de la Société de recherche opérationnelle.
22. "Kaizen: The Key to Japan's Competitive Success"par Masaaki Imai,edition McGraw-Hill Education,1986.
23. "The Toyota Way : 14 Management Principles from the World's Greatest Manufacturer" par Jeffrey K. Like,edition 2003.
24. "Implementing Enterprise Risk Management : Case Studies and Best Practices" par John Fraser et Betty J. Simkins,edition :Wiley, 2014.
25. "The Risk Management Process : Business Strategy and Tactics" par Christopher L. Culp, Edition Wiley 2001.

26. "La revue Communication et gestion des risques" par Vincent Gautrais et Yann Jodoin, professeurs titulaires à la Faculté de droit de l'Université de Montréal.
27. IFACI : Le Management des risques de l'entreprise, éditions d'organisation,2005.

Les articles

28. Institut des Auditeurs Internes (IIA) - Cadre International pour la Pratique Professionnelle de l'Audit Interne", disponible sur le site officiel de l'IIA.
29. Comité Basel sur la supervision Bancaire - Basel II : Convergence international sur mesure et normes de fonds propres : A version révisée
30. Risk Management and Insurance Review,
31. Journal of Risk and Insurance,
32. Institute of Risk Management (IRM),
33. Le Project Management Institute (PMI).

Les sites web :

1. https://www.theirm.org/
2. https://www.riskmanagementmonitor.com/
3. https://www.garp.org/
4. https://www.rims.org/

Les références légales et réglementaires en matière d'Audit et Risk Management :

1. ISO 31000 - Gestion des risques : les grandes lignes de la gestion des risques.
2. Loi Sarbanes-Oxley (SOX) : Loi américaine surveillance et contrôle des risques de fraude et anti-corruption dans le domaine des finances.
3. Normes Internationales pour la Pratique Professionnelle de l'Audit Interne (IPPF)
4. Normes Internationales d'Audit (ISA)

Table des matières

Remerciement

Sommaire..... I

Liste des abréviations..... II-III

Liste des tableaux..... IV

Liste des figures..... V

Résumé..... VI

Introduction Générale..... A-F

Chapitre 01 : L'Audit Interne ses appuis et ses conditions de mise en œuvres..... 1

Introduction du chapitre..... 2

Section 01 : Fondements de l'Audit Interne..... 3

1. Définitions et objectifs de l'Audit Interne..... 3
   - 1.1- Définition de l'Audit Interne..... 3
   - 1.2- Objectif de l'Audit Interne..... 4
     - 1.2.1- Evaluation du Contrôle Interne..... 4
     - 1.2.2- Gestion des risques..... 5
     - 1.2.3- Conformité aux politiques et procédures..... 6
     - 1.2.4- Amélioration des procédures opérationnels..... 7
     - 1.2.5- Gouvernance d'entreprise..... 9
     - 1.2.6- Communication des résultats..... 9
2. Normes et Cadre réglementaire..... 10
   - 2.1- Normes internationales pour la pratique professionnelle et l'Audit Interne..... 10
   - 2.2- Lois et réglementations locales..... 10
   - 2.3- Normes comptables..... 10
   - 2.4- Normes sectorielles..... 11
   - 2.5- Normes de gouvernance d'entreprise..... 11
3. Rôle et positionnement de l'Audit Interne dans l'organisation..... 11
   - 3.1- Rôle stratégique de l'Audit Interne..... 11
     - 3.1.1- Contrôle Interne..... 11

Table des matières

3.1.2- Conformité..... 11
3.1.3- Efficacité opérationnelle..... 12
3.1.4- Gestion des actifs..... 12
3.1.5- Gestion des projets..... 12
3.1.6- Prévention et détection de la fraude..... 12
3.1.7- Amélioration Continue..... 12
3.2- Positionnement de l'Audit Interne dans l'organisation..... 12
3.2.1- Indépendance et objectivité..... 12
3.2.2- Relation avec le Conseil d'Administration..... 13
3.2.3- Hiérarchie organisationnelle..... 13
3.2.4- Accès à l'ensemble de l'organisation..... 13
3.2.5- Coordination avec les autres fonctions de contrôle..... 13
3.2.6- Rapport réguliers..... 13
3.2.7- Evaluation de la performance..... 14
Section 02 : Appuis à l'Audit Interne..... 16
1. Soutien de la Direction et engagement de a Haute direction..... 16
1.1- Soutien financier et ressources..... 16
1.2- Crédibilité..... 16
1.3- Priorité stratégique..... 16
1.4- Culture d'intégrité et de responsabilité..... 17
1.5- Accès aux informations..... 17
1.6- Collaboration..... 17
1.7- Réponses aux recommandations..... 17
1.8- Formation continue..... 17
1.9- Mise en œuvre des recommandations..... 17
2. Ressources Humaines et compétences..... 18
2.1- Compétences techniques..... 18
2.2- Compétences en communication..... 18
2.3- Compétences en analyse et résolution de problèmes..... 19
2.4- Compétences en gestion de projet..... 19
2.5- Compétences en technologie de l'information..... 19

Table des matières

2.6- Compétences en éthique et intégrité..... 19
2.7- Compétences relationnelles..... 19
3. Technologies et Outils d'Audit..... 19
3.1- Logiciels d'audit automatisé..... 20
3.2- Système de gestion des audits..... 20
3.3- Analyse de données assistée par ordinateur (ADAO)..... 20
3.4- Technologie de collecte de données..... 20
3.5- Outils de gestion des risques..... 20
3.6- Logiciels de suivi des recommandations..... 20
3.7- Outils de communication et de présentation..... 20
3.8- Formation en ligne et module d'apprentissage..... 21
Section 03 : Conditions de mise en œuvre de l'Audit Interne..... 22
1. Planification et programmation des audits..... 22
1.1- Etablissement des objectifs de l'audit..... 22
1.2- Identification des domaines à auditer..... 22
1.3- Analyse des risques..... 22
1.4- Définition du plan d'audit..... 23
1.5- Allocation des ressources..... 23
1.6- Communication et engagement des parties prenantes..... 23
1.7- Elaboration d'un programme d'audit..... 23
1.8- Révision et approbation..... 23
2. Communication et rapports d'audit Interne..... 24
2.1- Importance de la communication efficace avec les parties prenantes..... 24
2.1.1- Transparence..... 24
2.1.2- Prise de décision éclairée..... 24
2.1.3- Gestion des attentes..... 24
2.1.4- Alignement avec les objectifs stratégiques..... 24
2.1.5- Réactivité aux préoccupation..... 24
2.2- Structuration des rapports d'audit et diffusion des résultats 25
2.2.1- Clarté et concision..... 25
2.2.2- Identification des risques et opportunités..... 25

Table des matières

2.2.3- Recommandations pratiques..... 25
3. Suivi et amélioration Continue..... 26
3.1- Clarté et compréhension..... 26
3.2- Identification des risques et opportunités..... 26
3.3- Recommandations pratiques..... 26
3.4- Suivi post-audit..... 26
3.5- Diffusion sélective..... 26
Conclusion du chapitre..... 27
Chapitre 02 : Le Risk Management..... 28
Introduction du chapitre..... 29
Section 01 : Aperçu sur le Risk Management..... 30
1. Généralité..... 30
1.1- Historique..... 30
1.1.1- Antiquité..... 30
1.1.2- Assurance Maritime au moyen âge..... 30
1.1.3- Assurance-incendie au XVIIe siècle..... 30
1.1.4- Développement de l'assurance au XVIIIe siècle..... 31
1.1.5- Révolution industrielle..... 31
1.1.6- Emergence de la gestion des risques d'entreprise (ERM) au XXe siècle..... 31
1.2- Normes et réglementations..... 31
1.3- Evolution numérique..... 31
1.4- Gestion des risques dans la finance..... 32
1.5- Le contexte normatif du Risk Management..... 32
1.5.1- ISO 31000 : 2018..... 32
1.5.2- COSO Entreprise Risk Management..... 32
1.5.3- BASEL III..... 32
1.5.4- Sarbanes-Oxley Act (SOX)..... 33
1.5.5- NIST Cybersecurity..... 33
1.5.6- Solvabilité II..... 33
2. Importance du Risk Management dans la prise de Décision..... 34
2.1- Anticipation des risques..... 34

Table des matières

2.2- Prise de décision éclairée..... 34
2.3- Optimisation des ressources..... 34
2.4- Protection de la réputation..... 34
2.5- Conformité réglementaire..... 34
2.6- Réduction des pertes financières..... 34
2.7- Planification stratégique..... 35
2.8- Amélioration de la réactivité..... 35
3. Objectif du Risk Management..... 35
3.1- Intégration dans la gouvernance et la culture de l'organisation..... 35
3.2- Prise de décision éclairée..... 35
3.3- Amélioration de la performance..... 36
3.4- Etablissement d'un processus continu..... 36
3.5- Adaptabilité et flexibilité..... 36
3.6- Communication et consultation..... 36
3.7- Alignement avec la stratégie..... 36
Section 02 : La démarche du Risk Management..... 37
1. Cadre de la gestion des risques..... 37
1.1-Contexte de l'organisation..... 37
1.2-Identification des risques..... 37
1.3-Analyse des risques..... 38
1.4-Evaluation des risques..... 38
1.5-Traitement des risques..... 38
1.6-Communication et consultation..... 38
1.7-Surveillance et revue..... 38
2. Méthode d'analyse des risques..... 39
2.1- Analyse SWOT..... 39
2.2- Analyse des causes à effets (Diagramme d'Ishikawa ou Fishbone)..... 41
2.3- Méthode PESTEL..... 42
2.4- Analyse des modes de défaillance et de leurs effets (AMDEC)..... 42
2.5- Analyse des 5P..... 42
2.6- Cartographie des risques..... 43

Table des matières

3. Amélioration Continue..... 45
3.1- Roue de Deming ou PDCA..... 46
3.2- Lean Management..... 47
3.3- Démarche Kaizen..... 47
3.4- Méthode des 6 Sigma..... 49
3.5- Les 7S de Mackinsey..... 50
Section 03 : Intégration du Risk Management dans la gestion d'entreprise..... 53
1. Incorporation du Risk Management dans la planification..... 53
1.1- Elaboration de scénarios..... 53
1.2- Intégration dans la planification stratégique..... 54
1.3- Planification opérationnelle..... 55
1.4- Mise en œuvre des plans de gestion des risques..... 55
2. Surveillance Continue des risques..... 56
3. Communication efficace sur les risques..... 56
Conclusion du chapitre..... 58
Chapitre 03 : Cas Pratique..... 59
Introduction du chapitre..... 60
Section 1 : Présentation de la Cible..... 61
1- Historique..... 61
2- Missions et Objectifs..... 62
2.1- Missions..... 62
2.2- Objectifs..... 63
3- Organisation..... 64
3.1- Direction Générale..... 64
3.2- Structure fonctionnelle..... 64
3.3- Structure opérationnelle..... 65
4- Les moyens de l'entreprise..... 66
4.1- Potentiel Humain..... 66
4.2- Infrastructure..... 66
4.3- Potentiel matériel..... 67
5- Motivation..... 67

Table des matières

Section 2 : Audit Interne du département de la sureté..... 68
1- Objectifs de l'Audit Interne de la sureté..... 68
2- Scope..... 68
3- Déroulement de la mission..... 69
3.1- Communication..... 70
3.2- Revue documentaire..... 70
3.3- Visites sur site..... 70
3.4- Sensibilisation..... 70
3.5- Consultation..... 70
3.6- Etablissement du programme d'Audit..... 71
3.7- Ressources utilisées..... 71
3.8- Analyse 71
3.8.1- Préparation des documents d'Audit..... 71
3.8.2- Réalisation des Audits..... 71
4- Résultats de la mission..... 72
4.1- Collecte des résultats..... 72
4.2- Identification des écarts 72
4.3- Evaluation des risques..... 74
4.4- Priorisation des actions correctives 74
5- Développement d'un plan d'action..... 76
6- Les résultats..... 78
7- Clôture de l'Audit..... 78
Section 3 : Audit Externe 79
1- Evaluation initiale..... 79
2- Formation et sensibilisation..... 79
3- Pré-Audit (facultatif) 79
3.1- Evaluation 79
3.2- Points d'améliorations..... 80
4- Audit de Certification..... 81
5- Rapport d'Audit Final..... 81
6- Actions Correctives 85

Table des matières

7- Certification…….. 85
8- Surveillance continue et audits de suivi…….. 85
Conclusion du chapitre…… 86
Conclusion Générale…….. 88
Bibliographie…….. 93
Table des matières…… 96