الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique

Ecole Nationale Supérieure de Management
Koléa

وزارة التعليم العالي و البحث العلمي

المدرسة الوطنية العليا للمناجمنت
القليعة

MÉMOIRE DE FIN D'ÉTUDES

En vue de l'obtention d'un Master académique en

« Management stratégique et système d'information »

Evaluation d'un cadre de gestion des risques de cybersécurité dans une approche de gouvernance IT

Cas pratique : Direction Générale de NAFTAL

Elaboré par :
KOUDJIL Zahra

Encadré par :
Dr. Himrane Mohammed

Année universitaire 2024/2025

Résumé

Dans un contexte de digitalisation croissante, les systèmes d'information sont devenus des leviers stratégiques pour les organisations, mais également des sources de vulnérabilités accrues. Les menaces telles que les violations de données, les interruptions de service ou les pertes financières rendent indispensable une gestion rigoureuse des risques liés à la cybersécurité. Cette étude vise à évaluer un cadre de gestion des risques cyber dans une perspective de gouvernance IT, à travers le cas de NAFTAL, entreprise publique algérienne spécialisée dans la distribution de produits pétroliers. L'objectif principal est d'analyser l'efficacité des pratiques actuelles de gestion des risques chez NAFTAL, en identifiant les menaces critiques, en évaluant les capacités organisationnelles et en formulant des recommandations adaptées. Pour cela, une méthodologie qualitative a été mobilisée, combinant une revue de littérature, des entretiens semi-directifs avec les responsables de la DSI, ainsi qu'une observation des pratiques sur le terrain. Les résultats montrent que NAFTAL est engagée dans une structuration progressive de sa gouvernance IT, avec des avancées notables en matière d'alignement stratégique. Toutefois, plusieurs faiblesses subsistent, notamment un déficit en ressources spécialisées, une coordination insuffisante entre départements, et une faible adoption des méthodes structurées comme MEHARI. Cette dernière, bien que conforme aux normes internationales, reste marginalisée du fait de sa complexité et d'un manque de formation. L'étude propose des mesures concrètes telles que la mise en place d'un comité cybersécurité, la standardisation des outils d'analyse des risques, et la formation continue. Elle ouvre enfin des perspectives pour étendre l'analyse à d'autres contextes organisationnels.

Mots-clés : Cybersécurité, gestion des risques, gouvernance IT, MEHARI, NAFTAL, systèmes d'information.

ABSTRACT

In a context of increasing digitalization, information systems have become strategic levers for organizations but are also sources of growing vulnerabilities. Threats such as data breaches, service disruptions, and financial losses make rigorous cybersecurity risk management essential. This study aims to evaluate a cyber risk management framework from an IT governance perspective, using the case of NAFTAL, a public Algerian company specialized in the distribution of petroleum products.

The main objective is to analyze the effectiveness of NAFTAL's current risk management practices by identifying critical threats, assessing organizational capabilities, and formulating appropriate recommendations. To this end, a qualitative methodology was adopted, combining a literature review, semi-structured interviews with IT department leaders, and direct observation of on-site practices.

The results show that NAFTAL is engaged in the gradual structuring of its IT governance, with notable progress in strategic alignment. However, several weaknesses persist, including a lack of specialized human resources, insufficient interdepartmental coordination, and limited adoption of structured methods such as MEHARI. Although compliant with international standards, MEHARI remains underutilized due to its perceived complexity and lack of training.

The study proposes concrete measures such as the establishment of a dedicated cybersecurity committee, the standardization of risk assessment tools, and the implementation of continuous training programs. It also opens up perspectives for extending the analysis to other organizational contexts.

Keywords: Cybersecurity, risk management, IT governance, MEHARI, NAFTAL, information systems.

الملخص

في ظل التحول الرقمي المتزايد، أصبحت نظم المعلومات روافع استراتيجية للمؤسسات، لكنها في الوقت ذاته أصبحت مصادر متزايدة للهشاشة. فالتهديدات مثل اختراق البيانات، وانقطاع الخدمات، والخسائر المالية تفرض ضرورة اعتماد إدارة صارمة للمخاطر المرتبطة بالأمن السيبراني. تهدف هذه الدراسة إلى تقييم إطار لإدارة المخاطر السيبرانية من منظور حوكمة تكنولوجيا المعلومات، من خلال دراسة حالة شركة نفطال، وهي مؤسسة عمومية جزائرية متخصصة في توزيع المنتجات البترولية.

يتمثل الهدف الرئيسي في تحليل فعالية ممارسات نفطال الحالية في إدارة المخاطر، من خلال تحديد التهديدات الحرجة، وتقييم القدرات التنظيمية، واقتراح توصيات مناسبة. لتحقيق ذلك، تم اعتماد منهجية نوعية جمعت بين مراجعة أدبية، ومقابلات شبه موجهة مع مسؤولي مديرية نظم المعلومات، بالإضافة إلى ملاحظة مباشرة للممارسات الميدانية.

أظهرت النتائج أن نفطال منخرطة في عملية تدريجية لبناء حوكمة تكنولوجيا المعلومات، مع تقدم ملحوظ في مجال التوافق الاستراتيجي. ومع ذلك، لا تزال بعض النقائص قائمة، لاسيما النقص في الموارد البشرية المتخصصة، وضعف التنسيق بين الأقسام، والاعتماد المحدود على الأساليب المنظمة مثل .MEHARI وعلى الرغم من توافق هذه الأخيرة مع المعايير الدولية، إلا أنها لا تُطبق بشكل واسع بسبب تعقيدها المُتصوَّر ونقص التكوين.

تقترح الدراسة تدابير عملية مثل إنشاء لجنة مخصصة للأمن السيبراني، وتوحيد أدوات تحليل المخاطر، وتطبيق برامج تكوين مستمر. كما تفتح آفاقاً لتوسيع التحليل ليشمل سياقات تنظيمية أخرى.

الكلمات المفتاحية: الأمن السيبراني، إدارة المخاطر، حوكمة تكنولوجيا المعلومات، MEHARI، نفطال، نظم المعلومات.

Remerciements

Avant tout, je tiens à exprimer ma profonde gratitude à Allah, Le Tout-Puissant, pour m'avoir accordé la force, la patience et la persévérance nécessaires à l'accomplissement de ce travail.

Je souhaite remercier du fond du cœur mes parents, Bouyahia et Khadidja, pour leur amour inconditionnel, leurs encouragements constants et leur soutien sans faille. Un hommage particulier à ma chère maman, pilier de ma vie, qui a toujours été présente pour moi. Je n'oublie pas mes frères Mohammed et Hakim, ainsi que mes sœurs Fatima, Fatiha, Rabiaa et Chaimaa, qui m'ont toujours soutenu avec affection. Une pensée toute particulière va à ma sœur Fatiha, qui a été un pilier pour moi dans les moments difficiles, notamment en assumant le rôle de notre défunt père – qu'Allah lui accorde, sa miséricorde et l'accueille en son vaste paradis. Que Dieu te protège Fatiha, et merci du fond du cœur.

Je tiens à exprimer ma reconnaissance à Docteur Himrane Mohammed, mon encadrant académique, pour son accompagnement, ses conseils avisés et sa disponibilité tout au long de ce travail.

Mes remerciements s'adressent également à toute l'équipe pédagogique et administrative de l'École Nationale Supérieure de Management (ENSM), pour la qualité de la formation dispensée et leur accompagnement. Une mention spéciale à Monsieur Belali Mounir, ancien directeur de l'ENSM, pour les efforts qu'il a déployés en faveur de notre promotion 2023–2025.

Je remercie chaleureusement Madame Amel Bourai (RSSI), mon encadrante professionnelle au sein de NAFTAL, pour son encadrement précieux, son soutien constant et sa grande disponibilité. Mes remerciements vont également à l'ensemble de l'équipe de la Direction Générale de NAFTAL, en particulier à la Direction des Systèmes d'Information (DSI), pour leur accueil, leur assistance et les conditions favorables à la réalisation de ce stage.

Enfin, je n'oublie pas tous mes amis, que ce soit au sein de l'école ou en dehors, pour leur amitié sincère, leur soutien moral et leur présence bienveillante durant cette aventure.

Table des matières

Liste des tableaux

Liste des figures

Liste des abréviations

ANSSI	Recommandations Nationales Françaises en Cybersécurité
CD	Comité de Direction
CISO	Chief Information Security Officer
COBIT	Control Objectives for Information and Related Technologies
CSF	Cybersecurity Framework
CSI	Comité de Sécurité de l'Information
DCSI	Direction Centrale des Systèmes d'Information
DG	Direction Générale
DSI	Direction des Systèmes d'Information
EGIT	Excellence en Gouvernance des Technologies de l'Information
ERM	Processus de gestion des risques intégrée
FAIR	Factor Analysis of Information Risk
GPL	Gaz de pétrole liquéfié
GRC	La gouvernance, les risques et la conformité
GSI	Gouvernance de la Sécurité de l'Information
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
IT	Technologies de l'information
ITIL	Information Technology Infrastructure Library
KPI	Indicateurs de performance clés
KRI	Indicateurs Clés de Risque
MEHARI	Management, Évaluation, Humain, Analyse, Réduction, Amélioration
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
PCI DSS	Payment Card Industry Data Security Standard
RGS	Référentiel Général de Sécurité
RSSI	Responsable de la Sécurité des Systèmes 9 d'Information

SI	Système d'information
SIEM	Security Information and Event Management
SLR	Revue systématique de la littérature
SMSI	Système de Management de la Sécurité de l'Information
SOC	Security Operations Center
SSI	Sécurité des systèmes d'information
UA	Union Africaine
UE	Union Européenne

INTRODUCTION

1. Contexte et objectif de la recherche

Dans un monde de plus en plus numérisé, les systèmes d'information sont devenus un élément stratégique des opérations organisationnelles. Ce qui était autrefois perçu comme un problème purement technique est désormais un composant clé de la gouvernance des technologies de l'information (IT). La nature dynamique et croissante des menaces cyber expose les organisations à des risques majeurs, tels que les violations de données, les interruptions de service, les atteintes à la réputation, voire des conséquences financières graves.

Face à ces défis, la gestion des risques liés à la cybersécurité est devenue une priorité pour les entreprises, notamment celles qui manipulent des données sensibles. C'est notamment le cas de NAFTAL, une grande entreprise algérienne spécialisée dans la distribution des produits pétroliers, dont les systèmes d'information doivent impérativement être protégés afin d'assurer la continuité de ses activités.

Cette recherche vise à évaluer un cadre de gestion des risques liés à la cybersécurité dans une approche de gouvernance IT. Elle cherche également à analyser dans quelle mesure les pratiques actuelles permettent à NAFTAL de détecter, évaluer et répondre aux menaces cyber en accord avec les exigences de gouvernance IT. L'objectif final est de proposer des recommandations opérationnelles afin de renforcer la posture de cybersécurité de NAFTAL en intégrant davantage la gestion des risques dans ses processus stratégiques.

2. Pertinence de la recherche

2.1 Pertinence théorique

D'un point de vue théorique, cette étude contribue à la recherche académique sur la gouvernance IT et la gestion des risques cyber en :

- Investigant les liens entre cybersécurité et gouvernance électronique ;
- Évaluant l'efficacité des outils d'analyse des risques (tels que la méthode **MEHARI**) dans un contexte organisationnel réel ;
- Approfondissant la compréhension des outils de contrôle et d'évaluation des risques en environnement informatique.

2.2 Pertinence managériale / pratique

Sur le plan managérial, l'étude offre des outils concrets et des connaissances utiles à la direction de NAFTAL en :

- Identifiant les menaces majeures en matière de cybersécurité qui pèsent sur ses systèmes d'information ;
- Évaluant le niveau actuel de maturité de la gestion des risques dans un cadre de gouvernance IT ;
- Optimisant ou adaptant la méthode de gestion des risques utilisée afin qu'elle réponde mieux aux besoins stratégiques ;
- Recommandant des indicateurs de performance clés (KPI) pour suivre l'efficacité de la gestion des risques dans la gouvernance IT de NAFTAL.

3. Problématique et questions de recherche

La problématique centrale à laquelle cette recherche souhaite répondre est la suivante :

Comment évaluer l'efficacité d'une stratégie de gestion des risques informatiques afin de permettre à NAFTAL d'améliorer la cybersécurité de ses systèmes d'information dans une approche de gouvernance IT ?

Cette question générale est déclinée en plusieurs sous-questions :

- Comment identifier les risques critiques de cybersécurité auxquels NAFTAL est exposée ?
- Comment évaluer la capacité actuelle de NAFTAL à gérer les risques informatiques dans une logique de gouvernance IT ?
- Comment adapter ou améliorer la stratégie de gestion des risques poursuivie par NAFTAL afin d'intégrer plus efficacement la cybersécurité dans son cadre stratégique ?
- Quels indicateurs de suivi peuvent être proposés pour mesurer l'efficacité de la gestion des risques dans la structure de gouvernance IT de NAFTAL ?

4. Plan de la recherche

Pour répondre à ces questions, la recherche est structurée comme suit :

- **Le premier chapitre** présente un cadre conceptuel et une revue de littérature, en définissant clairement les concepts fondamentaux relatifs à la cybersécurité, à la gouvernance IT et à la gestion des risques.
- **Le deuxième chapitre** détaille la méthodologie de recherche ainsi que le contexte organisationnel de NAFTAL, où l'étude a été réalisée.
- **Le troisième chapitre** expose les résultats issus du terrain, suivis d'une analyse approfondie et d'une discussion critique.

Enfin, la **conclusion** reprend les principaux résultats, présente les limites de l'étude, et propose des pistes de réflexion pour de futures recherches.

CHAPITRE Ⅰ: REVUE DE LA LITTERATURE ET CADRE CONCEPTUEL

1. Revue de la littérature

Dans un monde numérique en constante évolution, les problématiques de cybersécurité, de gestion des risques et de Gouvernance des Technologies de l'Information, Risques et Conformité (IT GRC) sont désormais au cœur des priorités stratégiques des organisations modernes. En se basant sur ces domaines d'étude et de pratique, cette revue identifie les travaux les plus significatifs qui ont émergé dans ces domaines, mettant en lumière les lacunes géographiques, les différences sectorielles et les actions entreprises par les organisations pour renforcer leur sécurité face aux cyberattaques. Les travaux analysés révèlent de grandes disparités entre les approches des États membres de l'Union Européenne (UE) et celles des pays de l'Union Africaine (UA), soulignant la nécessité d'une meilleure coordination régionale ainsi que de politiques harmonisées. De plus, les études sur la gestion des risques et l'intégration des systèmes d'information dans les politiques de cybersécurité soulignent le besoin d'une stratégie globale et coordonnée. Enfin, l'IT GRC émerge comme un paradigme essentiel pour l'harmonisation de la sécurité, de la conformité et de la performance au sein des organisations. Cette revue cherche à fournir un résumé des travaux récents et à identifier les principales lacunes de recherche afin de guider les études futures dans ces domaines complexes.

1.1. La cybersécurité dans le système d'informations

Le premier article de Abdelmadjid Ramdane met en évidence la grande disparité entre les politiques de cybersécurité adoptées par les États membres de l'Union européenne (UE) et celles mises en place par les pays de l'Union africaine (UA). L'étude souligne les avancées significatives de l'UE, rendues possibles grâce à des cadres réglementaires solides et élaborés, tels que la directive NIS, le Cybersécurité Act et le cadre NIST. En revanche, la majorité des pays africains sont confrontés à des difficultés persistantes, notamment un manque d'harmonisation des politiques, une pénurie de professionnels qualifiés et une coopération institutionnelle limitée. Ramdane plaide en faveur d'un renforcement des capacités et d'une coordination régionale accrue, afin de bâtir un écosystème de cybersécurité durable et collaboratif en Afrique. (Abdelmadjid, 2021)

Le deuxième article intitulé « Information System Approaches in Cybersecurity » de Prasetyo Adi Wibowo Putro, Eko Yon Handri et Dana Indra Sensuse, publié dans *Procedia Computer Science* (volume 234, 2024, pages 1372–1379), présente comme problématique centrale que, bien qu'il existe de nombreuses recherches en cybersécurité, l'application

spécifique des approches des systèmes d'information (SI) n'a pas été clairement identifiée. Les auteurs estiment qu'une approche systémique – prenant en compte les aspects techniques et socio-organisationnels – peut favoriser des fonctions clés de la cybersécurité telles que la dissuasion, la prévention, la détection et l'identification. Pour étayer cette hypothèse, ils ont mené une revue systématique de la littérature (SLR) portant sur 23 articles publiés entre 2017 et 2023, analysés selon les fonctions de cybersécurité et les composantes des SI (personnes, processus et technologies). Les résultats indiquent que les stratégies en SI, en particulier celles à dimension sociotechnique, jouent un rôle déterminant dans le renforcement des capacités en cybersécurité dans ces domaines d'activité. (Putro, 2024)

1.2. La gestion des risques en cybersécurité

Le premier article intitulé « A literature review of the factor that influence the adoption of an Enterprise Risk Management's process », écrit par Kerraous El Mehdi, enseignant-universitaire à l'Université Abdelmalek Essaâdi (Maroc), a pour objectif de déterminer les facteurs qui ont un impact sur l'adoption du processus de gestion des risques intégrée (ERM) dans les organisations. La problématique de base est : quels sont les facteurs qui poussent certaines organisations vers une adoption d'un ERM, et d'autres ne s'en investissent pas ? L'auteur émet 21 hypothèses basées sur la littérature, en supposant que des facteurs comme la présence d'un CRO, l'importance, la complexité ou bien l'indépendance du conseil d'administration ont une incidence positive sur l'adoption de l'ERM. La méthodologie repose sur une revue critique et structurée d'études empiriques antérieures menées à l'aide de méthodes telles que la régression logistique, des enquêtes, ou l'analyse de données publiques. Les résultats montrent que certains facteurs tels que la présence d'un CRO, la cotation en bourse, l'indépendance du conseil, le soutien du management, la présence d'un auditeur Big Four, la taille et la complexité ont une influence positive significative sur l'adoption de l'ERM. En revanche, diversification internationale est de nature négative, et toute autre variable comme la liquidité, la volatilité d'actions ou les économies d'impôt n'a pas d'impact significatif. L'étude est également en pointillé l'avènement de résultats contradictoires pour certaines variables pour inviter des futurs travaux. (KERRAOUS, 2020)

Le deuxième article de Pratik Sawant (KPMG) présente une approche globale de la gestion des risques en cybersécurité, conforme aux normes internationales telles que l'ISO 27001 :2013 et l'ISO 22301 :2012. Cette démarche s'articule autour des principales étapes que sont

l'identification, l'évaluation et le traitement des risques. L'auteur insiste sur l'importance d'adapter les contrôles de sécurité au profil de risque propre à chaque organisation, en combinant de manière réfléchie des mesures préventives, détectives et correctives. Par ailleurs, l'étude distingue différents types de risques — à savoir les risques inhérents, actuels (nets) et résiduels — et expose les stratégies de réponse possibles, telles que l'acceptation, la réduction, le transfert ou l'évitement des risques. (Lundgren, 2019). Le troisième article s'inscrit dans le cadre de l'initiative Sea4Value (ePilotage) sur l'automatisation maritime en Finlande, Pöyhönen et *al*. Étudient les risques liés aux échanges de données entre les navires et les services cloud. Ils adoptent une approche probabiliste permettant d'évaluer à la fois la probabilité de réussite des attaques et l'efficacité des mesures de protection, réparties en quatre grandes catégories : protection, détection, contre-mesures et reprise. Les résultats mettent en évidence la criticité des segments liés au cloud, identifiés comme les principales vulnérabilités du système (Pöyhönen, 2022)

La gouvernance IT et la gestion de risques

Dans un contexte de digitalisation croissante et de pressions réglementaires accrues, la Gouvernance, le Risque et la Conformité des Technologies de l'Information (IT GRC) s'imposent comme un levier essentiel pour atteindre une performance durable au sein des organisations modernes. Victor et al. (2024), dans leur article publié dans l'International Journal of Latest Technology in Engineering, Management & Applied Science, soulignent l'importance d'adopter une approche intégrée du concept IT GRC. Leur recherche met en évidence la manière dont ce modèle permet d'aligner les technologies de l'information avec les objectifs organisationnels, de renforcer l'excellence opérationnelle et de réduire l'exposition aux menaces et risques cybernétiques. L'étude identifie également une lacune théorique dans la littérature, suggérant la nécessité de recherches académiques supplémentaires sur la nature intégrée de l'IT GRC.

Conclusion

Les études analysées dans cette revue de littérature confirment que la cybersécurité, la gestion des risques et la gouvernance des technologies de l'information (IT GRC) doivent être abordées comme des enjeux stratégiques et globaux, englobant les dimensions techniques, humaines et organisationnelles. D'une part, l'Union européenne a fait des avancées significatives grâce à des cadres réglementaires stricts, tandis que l'Afrique continue de faire face à de nombreux défis, principalement le manque de coordination et le développement des compétences. D'autre part, l'intégration des systèmes d'information dans les contrôles de gestion des risques et de cybersécurité s'avère être un mécanisme crucial pour renforcer la sécurité des systèmes d'information. Enfin, l'IT GRC est un levier essentiel pour aligner les objectifs commerciaux et les technologies de l'information et traiter les questions complexes de sécurité. L'étude met en évidence l'importance d'une approche intégrée, proactive et contextuelle, en particulier dans des environnements aussi hétérogènes que ceux de l'UE et de l'UA.

2. Cadre conceptuel

2.1. Le système d'information

2.1.1. Définitions

Un système d'information est une collection structurée de ressources : équipements, programmes, équipes, données, procédures, etc., qui facilitent l'obtention, le traitement et le stockage d'informations (qu'il s'agisse de données, de textes, d'images, de sons, etc.) au sein et entre diverses organisations.

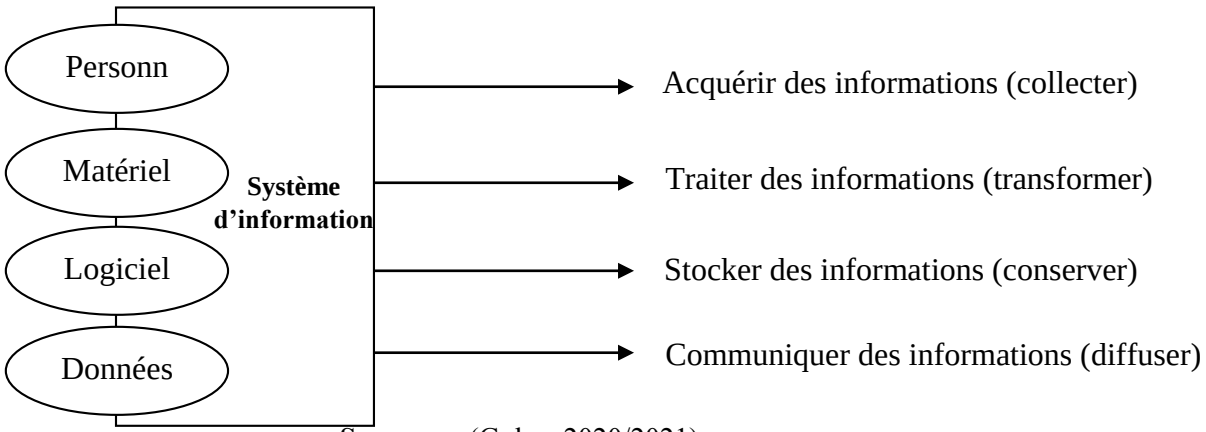
On peut donc caractériser le système d'information comme la totalité des flux d'informations qui circulent au sein de l'organisation, associés aux ressources déployées pour leur gestion (Reix, 2002)

L'automatisation se généralise de plus en plus au sein des systèmes d'information, signifiant que l'information est produite par des machines (automates et ordinateurs). Pour gérer les informations, tant les ordinateurs que les humains appliquent des normes et des processus. Par exemple, des algorithmes, des normes, des règlements, des procédures administratives ou encore des modèles mathématiques (Golea, 2020/2021)

Les fonctions d'un SI sont :

- **Acquisition :** La collecte d'informations par la saisie et/ou la consultation
- **Traitement :** Modification des données via des opérations informatiques ou des manipulations manuelles.
- **Stockage et mémorisation :** Consignation des données sur des supports.
- **Communication :** Le partage d'informations entre diverses personnes ou départements.

Figure 1 : Les fonctions d'un SI.



Sources : (Golea, 2020/2021).

2.1.2. Sécurité des systèmes d'information

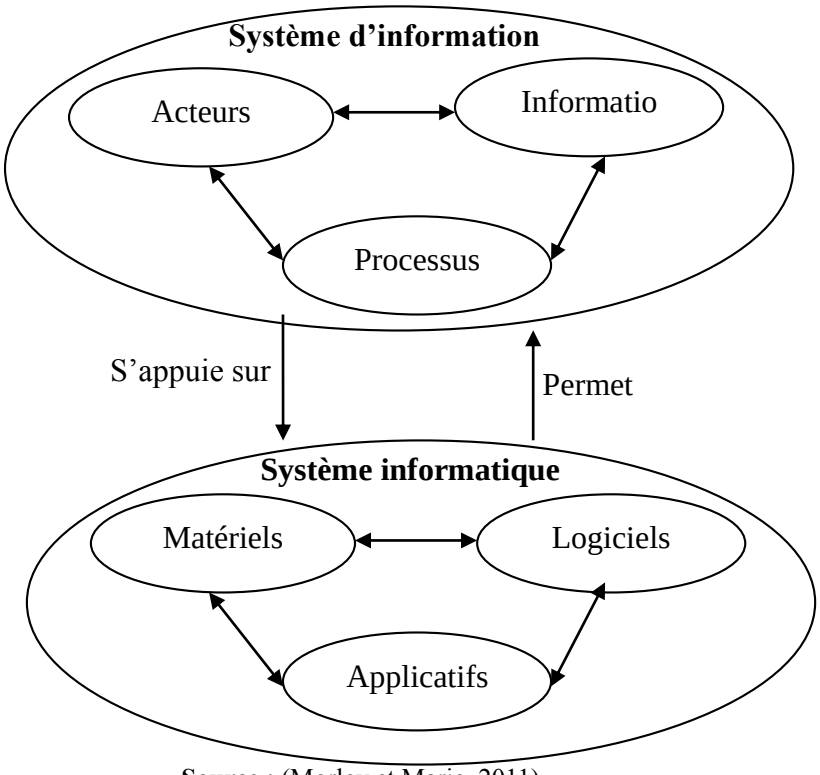
La sécurité peut être évaluer selon divers critères :

- **Disponibilité :** assurance que ces éléments pris en compte sont à la disposition des personnes habilitées au moment requis.
- **Intégrité :** Assurance que les informations prises en compte sont précises et exhaustives.
- **Confidentialité :** Assurance que seules les personnes ayant l'autorisation peuvent accéder aux éléments considérés.
- **Traçabilité ou preuve :** Assure que les accès et tentatives d'accès aux éléments concernés sont enregistrés, et que ces enregistrements sont stockés et utilisables.

Plusieurs scénarios sont envisagé s :

- Une méthode d'attaque (action ou événement, accidentel ou intentionnel).
- Les éléments qui représentent une menace (naturels ou humains, agissant de façon accidentelle ou intentionnelle)
- Les éléments potentiellement exploitables.
- Les failles des entités (matériels, logiciels, réseaux, organisations, personnels, locaux), qui peuvent être mises à profit par les éléments menaçants dans le cadre de la méthode d'attaque.

Figure 2 : Système informatique et système d'information.



Source : (Morley et Marie, 2011).

2.1.3. Les enjeux de la sécurité des SI

Le but de la sécurité est de minimiser les menaces qui pèsent sur le système d'information afin de minimiser leurs conséquences sur les opérations et les activités professionnelles des organisations. Pour cela divers enjeux doivent être maitrisés :

- **L'intégrité :** Les données doivent correspondre à ce qu'on attend d'elles, et ne pas être modifiées de manière accidentelle ou intentionnelle.
- **La confidentialité :** L'accès aux informations qui leur sont destinées n'est accordé qu'aux individus ayant reçu une autorisation. Il faut empêcher tout accès non autorisé.
- **La disponibilité :** Le système doit être opérationnel sans interruption pendant les périodes d'utilisation prévues, assurant l'accès aux services et ressources mises en place avec la réactivité attendue.
- **La non-répudiation et l'imputation** : Aucun utilisateur ne doit avoir la possibilité de nier les opérations qu'il a effectuées dans le cadre de ses actions permises, et personne d'autre ne doit pouvoir revendiquer les actions d'un autre utilisateur.
- **L'authentification :** La reconnaissance des utilisateurs est essentielle pour contrôler les accès aux lieux de travail appropriés et préserver la confiance dans les interactions commerciales.

La sécurité des systèmes informatiques est une problématique globale qui touche à divers aspects: les équipements matériels de traitement ou de transmission, les logiciels, les informations, ainsi que le comportement des utilisateurs. Le degré global de sécurité étant déterminé par le niveau de sécurité du maillon le plus faible, les mesures préventives et correctives doivent être prises en compte en fonction des vulnérabilités spécifiques au contexte pour lequel le système d'information est destiné à fournir service et soutien. (Boudriga, 2004)

La sécurité informatique

La sécurité informatique fait référence à toutes les mesures techniques, organisationnelles, juridiques et humaines nécessaires, ainsi que celles mises en œuvre, pour assurer la protection, la restauration et la garantie de la sécurité des systèmes informatiques. Elle est étroitement associée à la sécurité des systèmes d'information et de l'information. (Bloch, Sécurité informatique (3e éd.). Eyrolles., 2011)

La sécurité informatique est un processus continu qui a pour but de renforcer le niveau de sécurité en mettant en place une politique de sécurité au sein des organisations et en remédiant à certaines vulnérabilités tant organisationnelles que technologiques.

La sécurité des systèmes d'information (SSI) regroupe tous les moyens techniques, organisationnels, juridiques et humains requis et déployés pour préserver, restaurer et assurer la sûreté du système d'information. La garantie de la sécurité du système d'information relève des responsabilités de la gestion du système d'information.

Cette protection des systèmes informatiques favorise la qualité et garantit la défense des individus, des biens informationnels et des équipements face aux menaces internes et externes.

Les normes de sécurité de l'information facilitent l'établissement d'un véritable processus qualité dédié à la sécurité de l'information. Pour sa définition, son déploiement, son soutien et ses modifications, ainsi que pour son contrôle en vue de l'amélioration, il sera indispensable de disposer de ressources humaines, de solutions et de procédures. (Boudriga N. , 2004)

2.1. La cybersécurité

2.1.4. Définition de cybersécurité IT

Il s'agit d'un ensemble de méthodes et de technologies déployées pour non seulement défendre les actifs d'une entreprise contre les cyber-attaques, mais également pour réagir en cas d'atteinte à l'un de ces actifs, et restaurer leur fonctionnement normal suite à une attaque. La protection de l'image de l'entreprise fait également partie des enjeux liés à la Cybersécurité. (1., 2021/2022)

2.1.5. Dimensions de la cybersécurité IT

La cybersécurité IT est un domaine à multidimensionnelle qui cherche à défendre les systèmes d'information, les réseaux, les programmes et les informations contre des menaces de nature interne ou externe. Son accroissement de complexité nécessite une stratégie intégrale, organisée autour de plusieurs aspects complémentaires, chacun ayant un rôle crucial dans la sauvegarde de l'environnement numérique de l'organisation. (European Union Agency for Cybersecurity (ENISA), 2019)

2.2.2.1. La sécurité des données

La cybersécurité se concentre principalement sur la protection de la confidentialité, l'intégrité et la disponibilité des informations. Cet aspect a pour but de sauvegarder les informations sensibles, personnelles ou critiques contre : les divulgations d'informations, les modifications non autorisées (intégrité), et les incidents de perte d’accès ou les destructions (disponibilité). (European Union Agency for Cybersecurity (ENISA), 2021)

2.2.2.2. La sécurité des systèmes et des applications

Cette dimension se rapporte à la sécurisation des serveurs, ordinateurs, systèmes d'exploitation et applications professionnelles contre les failles logicielles, les cyberattaques ainsi que les configurations incorrectes. (Agence nationale de la sécurité des systèmes d'information (ANSSI), 2021)

2.2.2.3. La sécurité réseau

Son objectif est de garantir la sécurité des échanges de données sur les réseaux internes et externes.

La sécurité du réseau constitue une protection indispensable contre les agressions extérieures et les déplacements latéraux non autorisés au sein d'un système d'information. (Agence nationale de la sécurité des systèmes d'information (ANSSI), 2021)

2.2.2.4. La sécurité des identités et des accès (IAM)

L'administration des identités numériques et des droits d'accès constitue un élément essentiel de la cybersécurité informatique. Elle se base sur :

- Du moindre privilège (Least Privilege),
- Sur la séparation des responsabilités (SoD – Segregation of Duties),
- Et sur l'authentification multi-facteurs (MFA – Multi-Factor Authentication).

2.2.2.5. La supervision et la détection des incidents

Il est essentiel d'avoir la faculté de détecter, d'examiner et de répondre aux incidents de sécurité en temps réel. Cela implique :

- L'emploi de systèmes SIEM (Security Information and Event Management),
- La consolidation des journaux,
- L'implémentation de procédures de réponse aux incidents (SOC – Security Operations Center) est également réalisée.

Cette dimension est cruciale pour diminuer le délai de réponse et minimiser l'effet des incidents. (Agence nationale de la sécurité des systèmes d'information (ANSSI), 2021)

2.1.5. Typologie des menaces et vulnérabilités

2.1.5.1. Les menaces

La menace représente la possibilité inquiétante qu'un incident survienne, pouvant nuire à un système informatique. En d'autres termes, une menace est un événement ou une action qui pourrait compromettre la sécurité d'un système informatique. Les actions susceptibles de porter préjudice à un système informatique sont qualifiées de menaces informatiques. (Pillou, 2013)

Sur le plan de la sécurité informatique, les menaces peuvent découler de diverses actions provenant de différentes sources :

- **Origine opérationnel :** Ces menaces sont associées à l'état du système à un instant précis. Ceux-ci peuvent découler d'un défaut de programmation, d'une défaillance dans le filtrage des entrées utilisateur, d'un problème lié à la logique de traitement ou d'une erreur de paramétrage.
- **Origine physique :** Elles peuvent avoir une origine accidentelle, naturelle ou criminelle. On peut mentionner spécifiquement les catastrophes naturelles, les défaillances ou les dommages matériels, les incendies ou les interruptions d'alimentation électrique.
- **Origine humaine :** Ces menaces sont directement liées aux fautes humaines, que ce soit dans la création d'un système d'information ou dans sa façon d'être utilisé. Par conséquent, elles peuvent découler d'une faute de conception ou de configuration, tout autant que d'une insuffisance de sensibilisation des utilisateurs aux dangers associés à l'emploi d'un système informatique.

Voici les principales menaces possibles pour un système d'information :

- **Un utilisateur du système :** La grande majorité des incidents de sécurité dans un système d'information proviennent généralement d'un utilisateur négligent. Il ne souhaite pas compromettre l'intégrité du système sur lequel il œuvre, pourtant son attitude favorise le risque.
- **Une personne malveillante :** Un individu parvient à pénétrer dans le système, de manière légitime ou non, et peut ainsi accéder à des informations ou des programmes auxquels il ne devrait pas avoir accès. Il est courant d'utiliser des programmes au sein du système, mais qui sont mal protégés.
- **Un programme malveillant :** Un programme conçu pour causer du tort ou exploiter les ressources du système a été installé sur le système, ce qui pourrait permettre des intrusions ou modifier les informations. Il se peut que des informations sensibles soient recueillies à l'insu de l'utilisateur et exploitées dans un but nuisible.

- **Vulnérabilité :** Dans le secteur de la cybersécurité, une vulnérabilité ou faille représente une faiblesse au sein d'un système informatique qui autorise un attaquant à compromettre l'intégrité du système, soit son fonctionnement standard, ainsi que la confidentialité et l'intégrité des informations qu'il renferme. (Pillou, 2013)

Exemples de vulnérabilités :

Voici quelques-unes des vulnérabilités les plus connues :

- Dépassement de tampon.
- Injection SQL.
- Cross site scripting.

- **Qu'est-ce qui rend les systèmes vulnérables ?**

- La sécurité est coûteuse et complexe, et certaines entreprises manquent de fonds pour sa mise en application.
- Il est impossible d'avoir une sécurité à 100% et elle s'avère souvent peu efficace.
- Les organisations sont prêtes à prendre des risques, la sécurité n'est pas leur préoccupation principale.
- Des technologies inédites (et par conséquent des vulnérabilités) voient constamment le jour.
- Les systèmes de sécurité sont conçus, administrés et paramétrés par des individus.
- Aucune infrastructure n'est en place pour les clés et autres composants de cryptographie.

- **Publication d'une vulnérabilité :**

L'approche de publication des vulnérabilités est une question qui suscite des discussions au sein de la communauté dédiée à la sécurité des systèmes d'information. Il y en a qui soutiennent qu'il est indispensable de publier intégralement toutes les informations concernant une vulnérabilité dès sa découverte. Certains suggèrent qu'il serait préférable d'abord de restreindre la diffusion à ceux qui en ont un besoin crucial, puis après une période déterminée, de rendre l'information accessible en détail, si nécessaire.

Ces périodes peuvent offrir aux développeurs l'occasion de rectifier la vulnérabilité et à leurs utilisateurs d'installer les correctifs de sécurité indispensables. Cependant, cela peut également augmenter le danger pour ceux qui ne sont pas au courant de ces informations (Jean-François et Jean, 2013). Cette approche de publication est qualifiée de « divulgation responsable » par les développeurs de logiciels, qui incitent les experts en sécurité à l'adopter (Bloch L. &., 2011)

2.1.6. Les référentiels de cybersécurité IT

2.2.4.1. ISO/IEC 27001 – Système de Management de la Sécurité de l'Information (SMSI)

- **Objectif** : Cette norme internationale définit les exigences pour la mise en place, l'exploitation, le maintien et l'amélioration continue d'un Système de Management de la Sécurité de l'Information (SMSI).
- **Approche** : Elle repose sur une méthodologie de gestion des risques visant à garantir la confidentialité, l'intégrité et la disponibilité des informations au sein d'une organisation.
- **Structure** : Elle comprend des politiques, des procédures et des contrôles spécifiques, ainsi que des processus d'audit et de revue récurrents pour assurer une amélioration continue.

2.2.4.2. ISO/IEC 27005 – Gestion des Risques liés à la Sécurité de l'Information

- **Objectif** : Cette norme complète l'ISO/IEC 27001 en fournissant une méthodologie détaillée pour gérer les risques en matière de sécurité de l'information.
- **Approche** : Elle aide les organisations à identifier, évaluer et traiter les risques sur la base d'une compréhension claire de leur environnement organisationnel et de leur tolérance au risque.
- **Avantage** : L'ISO 27005 est flexible et permet aux organisations d'adapter les procédures de gestion des risques à leur configuration opérationnelle propre.

2.2.4.3. NIST Cybersecurity Framework (CSF)

- **Objectif** : Développé par le National Institute of Standards and Technology (NIST) des États-Unis, ce cadre vise à aider les organisations à gérer et à atténuer les risques cyber.
- **Structure** : Le cadre repose sur cinq fonctions clés :
  - **Identifier** : Comprendre le contexte métier, les systèmes et les actifs.
  - **Protéger** : Mettre en œuvre des mesures de protection pour sécuriser les actifs et services.
  - **Détecter** : Mettre en place des activités pour identifier les incidents de cybersécurité.
  - **Répondre** : Réagir de manière appropriée aux incidents identifiés.
  - **Rétablir** : Maintenir des plans de résilience et restaurer les capacités après une violation.

- **Flexibilité** : Ce cadre est largement utilisé dans les secteurs public et privé, et peut s'adapter à divers secteurs et tailles d'organisation.

2.2.4.4. COBIT (Control Objectives for Information and Related Technologies)

- **Objectif** : COBIT est un cadre de gouvernance et de gestion des technologies de l'information permettant d'aligner la stratégie IT sur les objectifs métier.

- **Composante sécurité** : Il comprend des processus spécifiques à la sécurité de l'information, notamment le processus "DSS05 : Gérer la sécurité", qui traite de la gestion des risques, des accès et des incidents.

- **Valeur ajoutée** : COBIT est particulièrement utile pour intégrer la cybersécurité dans la gouvernance globale des TI et les stratégies de gestion des risques de l'entreprise.

2.2.4.5. ITIL (Information Technology Infrastructure Library)

- **Objectif** : ITIL fournit des meilleures pratiques pour la gestion des services informatiques, en mettant l'accent sur l'alignement des services IT aux besoins métiers.

- **Lien avec la cybersécurité** : Bien qu'il ne s'agisse pas d'un référentiel spécifique à la cybersécurité, ITIL inclut des processus essentiels tels que la gestion des incidents, des problèmes, et de la continuité de service, qui jouent un rôle important en matière de sécurité des systèmes d'information.

- **Avantage** : ITIL permet de structurer les opérations IT pour les rendre plus efficaces et réduire les vulnérabilités causées par une mauvaise gestion des services.

2.2.4.6. PCI DSS (Payment Card Industry Data Security Standard)

- **Objectif** : PCI DSS est une norme de sécurité de l'information destinée aux organisations qui traitent, stockent ou transmettent des données de cartes de paiement.

- **Exigences clés** : Elle impose des contrôles d'accès stricts, la segmentation des réseaux, le chiffrement des données et des politiques de sécurité.

- **Conformité** : Obligatoire pour les entreprises qui traitent des paiements, elle vise à prévenir les violations de données et à protéger les informations des détenteurs de cartes.

2.2.4.7. ANSSI – Recommandations Nationales Françaises en Cybersécurité

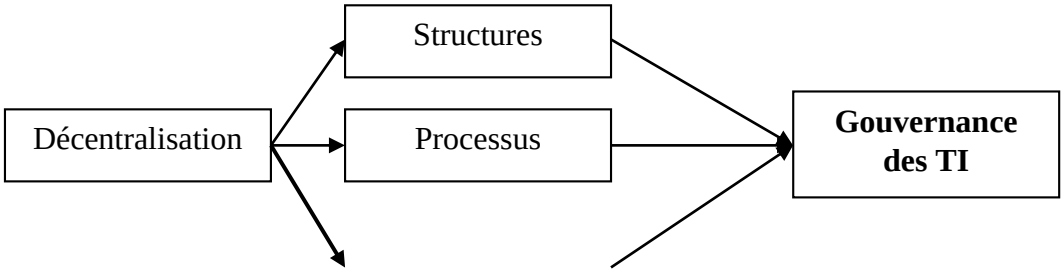
- **Objectif** : L'ANSSI (Agence nationale de la sécurité des systèmes d'information) fournit des recommandations nationales en matière de cybersécurité, notamment pour les entités du secteur public en France.
- **Référentiels** : Sa contribution majeure est le Référentiel Général de Sécurité (RGS), qui définit les exigences de sécurité pour les systèmes d'information publics.
- **Contenu** : Le RGS couvre l'analyse des risques, l'authentification des utilisateurs, la confidentialité des données et la disponibilité des systèmes. (International Organization for Standardization, 2022; ISO/IEC, 2022; International Organization for Standardization, 2018; National Institute of Standards and Technology, 2024; ISACA, 2012; AXELOS, 2019; Payment Card Industry Security Standards Council, nd; ANSSI, 2010)

2.2.Gouvernance IT

2.2.1. La gouvernance IT, son importance et ses objectifs

La gouvernance des TI est un concept apparu dans les années 90. Elle s'est transformée en un outil crucial pour une variété d'organisations. Ainsi, des études ont été menées consécutivement pour analyser ce concept, ses mécanismes et ses dimensions avec précision. Selon la définition donnée par l'Institut de gouvernance des technologies de l'information ((ITGI), 2001), la gouvernance des technologies de l'information est une responsabilité qui incombe au conseil d'administration et à la direction générale. Elle est un élément essentiel de la gouvernance d'entreprise, comprenant des structures et des processus organisationnels qui soutiennent et étendent les stratégies et les buts de l'organisation. Quant à eux, De (Haes, 2009) définissent la gouvernance des TI comme «un élément essentiel de la gouvernance d'entreprise géré par le conseil d'administration, impliquant l'établissement et l'application des processus, structures et mécanismes relationnels au sein de l'organisation qui autorisent les individus en charge des rôles techniques et informatiques à remplir leurs fonctions afin de favoriser l'harmonisation entre métiers et TI et à générer la valeur métier grâce aux investissements dans les TI». (Weill, 2004)

Figure 3 : Modèle conceptuel adopté.



Mécanismes relationnels

Source : Adapté de De Haes et Van Grembergen (2004).

Selon **(Howard, 2023)**, les objectifs principaux de la gouvernance informatique sont :

- **Adapter les IT/SI aux buts stratégiques de l'entité** : La gouvernance informatique doit assurer que les investissements en systèmes d'information et technologie de l'information sont en adéquation avec les buts stratégiques de l'entité et apportent de la valeur ajoutée à l'entreprise.
- **Gérer les risques associés aux IT/SI** : Les systèmes d'information et de technologie sont confrontés à différents types de risques, notamment les menaces informatiques, les défaillances de système et les fautes humaines. Il est essentiel que la gouvernance IT permette de repérer, d'apprécier et de minimiser ces dangers.
- **Optimiser les couts des IT/SI** : La gouvernance informatique doit aider à rationaliser les coûts en s'assurant que les ressources sont exploitées de façon optimale et efficiente.
- **Augmenter l'efficacité opérationnelle des SI/IT** : La gouvernance IT doit contribuer à augmenter l'efficacité opérationnelle des SI/IT en perfectionnant les procédures et en assurant la qualité des services technologiques.
- **Promouvoir l'innovation via les SI/IT** : La gouvernance IT doit favoriser un climat d'innovation en aidant les entreprises à exploiter les technologies émergentes pour concevoir de nouveaux produits et services.

2.2.2. Les activités de gouvernance

- **Surveiller :** Les dirigeants contrôlent les performances en se servant de systèmes d'évaluation appropriés et s'assurent qu'elles sont conformes aux stratégies et aux buts de la société.
- **Evaluer :** Les décideurs examinent l'usage présent et futur des technologies de l'information, en prenant en considération le progrès technologique, les tendances économiques et sociales, ainsi que les restrictions politiques et juridiques.
- **Diriger :** Les responsables attribuent les tâches relatives à l'élaboration et la mise en application des stratégies et directives liées aux technologies de l'information, qui déterminent les investissements à effectuer pour les projets et les services à proposer. Ils s'assurent que la stratégie est transmise de façon efficace au niveau de la direction et du management. (Bawden, 2019)

2.2.3. Avantage de gouvernance

Selon **l'ISACA (2020),** l'Excellence en Gouvernance des Technologies de l'Information (EGIT) met l'accent sur deux axes essentiels : la génération de valeur et le contrôle des risques associés à la transition numérique. Cette démarche cherche à optimiser les bénéfices de l'Information et de la Technologie (I&T) tout en réduisant les risques commerciaux liés. Cela se manifeste par trois résultats principaux :

- **Optimisation des avantages :** L'EGIT s'efforce de générer de la valeur pour l'entreprise en coordonnant étroitement les investissements dans l'I&T avec les buts stratégiques. Cela nécessite de préserver et d'augmenter la valeur des investissements en cours, tout en supprimant les projets qui ne génèrent pas assez de valeur. On met l'accent sur la fourniture de services et solutions informatiques sur mesure, dans le respect des délais et du budget alloué, tout en évaluant l'impact financier et non financier de ces actions.
- **Gestion optimisée des risques** : L'EGIT a pour objectif de déceler, d'apprécier et de maîtriser les risques commerciaux liés à l'I&T. Ceci englobe les dangers associés à l'usage, la possession, l'exploitation, l'engagement et l'intégration des I&T au sein de l'entreprise. Cette gestion des risques est insérée dans la stratégie globale de gestion des risques de l'entreprise afin d'assurer la conservation de sa valeur commerciale. On évalue les avancées dans ce secteur afin de prouver l'influence de l'optimisation des risques sur la performance générale de la société.
- **Amélioration des ressources** : L'EGIT veille à ce que les ressources requises soient disponibles pour mettre en œuvre efficacement le plan stratégique de la société. Cela englobe la mise en place d'une infrastructure informatique intégrée et rentable, l'implémentation de nouvelles technologies en fonction des exigences de l'entreprise, ainsi que la préservation des compétences du personnel IT. L'optimisation des ressources nécessite également une utilisation efficace des données et des informations.

2.3.La gestion de risque

2.3.1. Définitions

Le risque est défini par la formule suivante : (Sebri, 2022)

Risque = (Menace x Vulnérabilité) /Contre-mesures

Menace= Violation potentielle d'une propriété de sécurité.

Le domaine de la gestion des risques englobe l'identification, l'évaluation et le traitement des risques. La reconnaissance des risques liés à l'infrastructure de sécurité existante aide les entreprises à repérer les faiblesses et les dangers, ainsi que les menaces que ces éléments posent pour leur système de protection. L'évaluation des risques consiste à examiner les risques identifiés en tenant compte d'éléments comme la probabilité et l'influence, tandis que la gestion des risques vise à diminuer leur incidence à un niveau tolérable. (eSecurity Solutions, 2019)

Principes fondamentaux de la gestion des risques de sécurité IT

2.3.1.1. Identification des actifs et des risques

L'identification des risques consiste à repérer les dangers associés à la sûreté de l'information.

Le risque représente la possibilité qu'un incident défavorable survienne et entraîne des effets négatifs pour l'entité. Le processus d'identification des risques se divise en deux aspects majeurs : la détection des vulnérabilités et celle des menaces.

Les vulnérabilités se définissent comme des points faibles ou des insuffisances dans la structure de sécurité. (CDW, 2017)

Les vulnérabilités peuvent être d'ordre technique ou découler de failles dans les procédures de sécurité. Le manque de programme antivirus, l'autorisation d'accès sans restriction pour les utilisateurs, l'absence de responsables de la sécurité, et ainsi de suite. Les vulnérabilités des processus organisationnels incluent le manque de contrôle des historiques judiciaires, l'absence de procédure de gestion des modifications pour gérer les modifications apportées à l'infrastructure informatique essentielle, ...ect.

Le risque est l'issue ou l'effet néfaste qui se produit lorsqu'une menace exploite une vulnérabilité.

2.3.1.2. Déclaration de risque

Il existe une menace d'incendie dans les installations de la société si des extincteurs additionnels ne sont pas mis en place, ce qui pourrait causer des dégâts aux infrastructures et nuire au personnel. Dans l'énoncé du risque précité, l'incendie est le danger qui capitalise sur la faiblesse due à l'absence d'extincteurs et engendre des répercussions défavorables pour l'organisation, y compris des détériorations aux installations et des préjudices aux salariés. Il est conseillé d'effectuer une évaluation des risques annuellement ou lors de tout changement dans la posture de sécurité de l'organisation. (Sawant, 2020)

2.4.2.3. Évaluation du risque (analyse de l'impact et de la probabilité)

L'évaluation des risques est le processus d'analyse des risques. Lors de l'évaluation du risque, il est essentiel de considérer la probabilité et l'impact comme des éléments clés. Le degré total d'exposition au risque se réfère à la probabilité qu'un incident regrettable survienne, multiplié par les conséquences ou les préjudices éventuels causés par cet incident.

La probabilité représente la probabilité qu'une menace exploite une vulnérabilité sur une période donnée. Plus le risque d'exploitation d'une vulnérabilité est grand, plus la menace est importante. De même, l'impact se réfère à la sévérité des conséquences que l'organisation devra affronter si le risque se concrétise. Plus la gravité des conséquences est importante, plus le risque tend à être grand. (Sawant, 2020)

2.1.1.1. Traitement des risques (réduction, acceptation, transfert, évitement)

Il est nécessaire d'identifier et de mettre en place des vérifications pour réduire les risques détectés. L'identification et la mise en œuvre de ces éléments nécessitent une évaluation coûts-avantages. Cette évaluation assure que le coût d'implémentation des contrôles ne surpasse pas les dépenses encourues suite à la réalisation du risque. On distingue trois sortes de contrôles : les contrôles de détection, les contrôles préventifs et les contrôles correctifs. (NIST, 2018)

Les contrôles de détection identifient la menace à temps et informent l'administrateur pour qu'il puisse la neutraliser avant que la vulnérabilité soit exploitée. Les mesures de prévention font obstacle à toute tentative d'intrusion dans le système. Les mesures correctives permettent de mener une enquête sur les causes fondamentales pour empêcher la menace d'exploiter à nouveau la vulnérabilité.

Dans le cadre d'une activité d'évaluation des risques, on distingue plusieurs formes de risques : le risque inhérent, le risque brut, le risque net et le risque résiduel. (Sawant, 2020)

Pour gérer les risques, les entités doivent déterminer un seuil de risque jugé acceptable. On peut déterminer cette valeur en examinant la posture de sécurité de l'information de l'organisation, les besoins des clients, les obligations réglementaires et la perspective de la direction. On peut accepter les risques dont la valeur nette est inférieure à la valeur acceptable. Il est impératif pour les organisations de garantir que la valeur du risque résiduel reste en dessous du seuil acceptable. La gestion des risques nécessite l'élaboration d'un plan de traitement. Ce dispositif intègre des stratégies de gestion des risques comme l'acception, l'évitement, l'atténuation et la cession du risque.

La réduction du risque implique la mise en place de nouveaux mécanismes de contrôle pour minimiser à un niveau acceptable leur probabilité et leur impact. Le transfert du risque implique la cession de ce dernier à une partie tierce afin de compenser les frais ou les conséquences encourus suite à sa réalisation. Un cas de transfert de risque est l'assurance. Avant l'application du plan de gestion des risques, il est indispensable de consulter le RSSI ainsi que les chefs de département. (Sawant, 2020)

2.1.2. Les risques liés aux cybersécurité IT

La cybersécurité IT doit faire face à divers dangers qui mettent en péril la confidentialité, l'intégrité, la disponibilité et la traçabilité des systèmes d'information et des données. Ces menaces peuvent engendrer des répercussions sérieuses sur les opérations d'une entité, y compris l'interruption de service, l'érosion de la confiance, les sanctions réglementaires ou encore des pertes financières. (Khidzir, 2018)

On peut classer les risques en différentes catégories majeures : (Caralli, 2012)

2.4.3.1. Risques d’accès non autorisé (Violation de la confidentialité)

- Accès non autorisés aux systèmes par le biais de comptes compromis, l’ingénierie sociale ou des vulnérabilités logicielles.
- Accès non autorisé à des informations sensibles (ressources humaines, clients, financières, stratégiques).
- Vol de secrets commerciaux ou divulgation d'informations sensibles.

2.4.3.2. Risques de modification ou de disparition des données (Violation de l’intégrité)

- Altération non autorisée ou accidentelle des données.
- Corruption de bases de données due à une défaillance logicielle ou à une attaque.

- Éliminations malveillantes ou irréversibles.

2.4.3.3. Risques de non-disponibilité (Violation de la disponibilité)

- Dysfonctionnements matériels ou logiciels non prévus.
- Les attaques par déni de service distribué (DDoS) entraînent une interruption des services en ligne.
- Des ransomwares qui cryptent les systèmes et entravent l'accès aux informations.

2.4.3.4. Risques associés au facteur humain

- Problèmes de configuration ou de gestion.
- Négligence des utilisateurs (mots de passe faibles, clics sur pièces jointes infectées).
- Utilisation inappropriée des privilèges d'accès.

2.4.3.5. Risques associés aux vulnérabilités techniques

- Bugs dans le logiciel qui n'ont pas été rectifiés.
- Manque de mises à jour ou de corrections (gestion des correctifs défaillante).
- Systèmes obsolètes (end-of-life) toujours en fonctionnement.

2.4.3.6. Risques associés aux tiers (supply chain)

- Recours à des fournisseurs ou sous-traitants de services informatiques (cloud, maintenance, … etc.).
- L'intégration de programmes tiers comportant des vulnérabilités.
- Manque de maîtrise sur les accès et les procédures de sécurité des partenaires. (Caralli, 2012)

2.1.3. Outils et méthode d'analyse le risque IT

L'évaluation du risque en matière de cybersécurité IT s'appuie sur des techniques rigoureuses et des instruments spécialisés pour détecter, mesurer et classer les menaces qui pèsent sur le système d'information. L'intention est d'appuyer le processus décisionnel et de mettre en œuvre des actions de sécurité proportionnelles au degré de risque. **(Agence nationale de la sécurité des systèmes d'information, 2010)**

2.4.4.1. Méthodes d'analyse du risque IT

a) Analyse qualitative

- S'appuie sur un jugement subjectif de la sévérité du risque, en fonction de l'expertise, des conseils des spécialistes et des matrices d'évaluation.
- Exploite des gradations (bas / moyen / haut) pour évaluer l'impact et la chance.
- Bénéfices : vitesse, coût abordable, appropriée pour des contextes complexes ou mal documentés.
- Désavantages : moins précise, repose fortement sur l'interprétation des analystes.

b) Analyse quantitative

- Évalue les risques en termes quantitatifs : risque financier potentiel, fréquence annuelle de survenance, coût de gestion, … etc.
- Favorise des décisions budgétaires plus exactes.
- Limitations : requiert des données passées de confiance et une expertise approfondie.

c)Analyse combinée

- Emploie aussi bien des aspects qualitatifs que quantitatifs pour une évaluation plus équilibrée.
- C'est le modèle fréquemment choisi par les grandes entreprises. (ISACA, 2021)

2.4.4.2. Outils d'analyse du risque IT

Les outils offrent la possibilité de structurer, centraliser et documenter les évaluations de risques de façon organisée. Voici quelques instruments fréquemment employés : (Agence nationale de la sécurité des systèmes d'information, 2010)

a) Gestionnaire de Risques EBIOS (ANSSI)

- La méthode officielle française pour l'évaluation des risques dans le domaine de la cybersécurité.
- Recommandée pour les administrations, OIV (Opérateurs d'Importance Vitale), et entreprises critiques.
- Organise l'analyse en fonction des événements craints, des origines de menace, des scénarios menaçants, des mesures déjà en place, … etc.
- Source officielle.

b) MEHARI (CLUB de la sécurité de l'information français – CLUSIF)

- Méthode open source pour la gestion des risques axée sur les actifs, les vulnérabilités et les impacts métier.
- Propose des matrices d'évaluation et un guide d'analyse.
- Conçue pour l'automatisation à l'aide de tableurs ou d'outils internes.

c) OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

- Élaborée par le CERT (États-Unis).
- Se concentre sur la compréhension sectorielle, l'importance des actifs et l'examen des scénarios de menace.
- Approche qualitative axée sur la gestion. (Alberts, 2002)

d) FAIR (Factor Analysis of Information Risk)

- Une méthode quantitative standardisée par l'Open Group.
- Employée par les grandes sociétés pour la modélisation financière des cyber-risques.
- Adapté pour les instruments de GRC (Gouvernance, Risque et Conformité). (The Open Group, 2013)

e) Logiciels de gestion des risques ou de cybersécurité intégrée

- Risk Manager (de MEGA), RiskWatch, Archer, ISO Risk Manager, …ect.
- Comprennent fréquemment : l'inventaire des actifs, la cartographie des risques, les plans d'intervention, les rapports de conformité.
- Employés au sein de grandes entreprises et d'administrations pour une gestion centralisée. (ISACA, 2021)

2.4.4.3. Étapes typiques d'une analyse de risque IT

a) Identification des actifs essentiels à sécuriser
b) Appréciation des menaces et des vulnérabilités,
c) Évaluation du degré de risque (impact × probabilité),
d) Traitement des risques (diminution, transfert, acceptation, évitement),
e) Suivi et réévaluation régulière. **(Organisation internationale de normalisation, 2022)**

2.1.4. Processus

L'ensemble du processus de gestion des risques informatiques représente la colonne vertébrale de toute stratégie de cybersécurité performante. Il permet de repérer, d'évaluer, de

gérer et de surveiller les risques susceptibles d'affecter la sûreté du système d'information. Cette procédure s'aligne sur un processus itératif et constant, conformément aux normes internationales telles que l'ISO/IEC 27005, l'ISO 31000 ou le cadre de gestion des risques du NIST. Ce processus se compose généralement des étapes suivantes :

2.4.5.1. Définition du contexte

- Compréhension du cadre organisationnel, technique et réglementaire.
- Identification des objectifs opérationnels, des exigences de conformité et des problématiques de sécurité.
- Établissement des frontières de l'analyse (système global, application, projet, …etc.).

2.4.5.2. Reconnaissance des actifs, des menaces et des vulnérabilités

- Recensement des actifs informationnels (données, serveurs, applications, utilisateurs, … etc.).
- Identification des menaces éventuelles (internes, externes, humaines, naturelles, techniques).
- Évaluation des vulnérabilités susceptibles d'être utilisées par ces menaces.

2.4.5.3. Évaluation des risques

- Évaluation du niveau de risque en mettant en relation : la probabilité que la menace se produise et l'impact potentiel si cela se réalise.
- Catégorisation des risques basée sur une matrice de criticité (léger, modéré, majeur, critique).

2.4.5.4. Traitement du risque

- Établissement d'une stratégie de gestion :

- **Réduction** : implémenter des mesures de sécurité.
- **Transfert** : assurance ou délégation.
- **Acceptation** : si le risque est considéré comme résiduel ou tolérable.
- **Évitement** : renoncement ou changement de l'activité à risque.

- Mise en place d'une stratégie de gestion des risques comprenant des actions, des délais et des personnes en charge.

2.4.5.5. Suivi et réévaluation

- Établissement d'indicateurs de suivi (KRI - Indicateurs Clés de Risque).
- Évaluation périodique des risques basée sur :

- Des progrès technologiques.
- Des incidents survenus.
- Des modifications organisationnelles.

- Actualisation du registre des risques.

2.4.5.6. Communication et documentation

- Dialogues fréquents avec les intervenants (direction, départements, sécurité, informatique).
- Suivi des décisions, résultats d'analyse et stratégies d'action.
- Inscription du processus au sein de la gouvernance globale en matière de sécurité. **(ISO/IEC, 2022)**

2.2.MEHARI

La sécurité du système d'information est essentielle pour chaque entreprise, étant donné qu'un dysfonctionnement peut provoquer des effets catastrophiques, comme la dégradation de sa réputation, le piratage de ses secrets industriels ou la disparition de données essentielles, pouvant potentiellement conduire à sa banqueroute. Afin d'assurer cette protection, les gestionnaires informatiques ont à leur disposition plusieurs techniques comme EBIOS, MEHARI, MARION, MELISA, OCTAVE. Ces approches leur offrent des structures et des procédures pour mettre en place une politique de sécurité solide et effectuer des vérifications pour contrôler son efficacité. La mise en place de la sécurité informatique peut s'avérer complexe, cependant ces techniques sont élaborées dans le but de simplifier ce processus et d'assurer une défense appropriée du système d'information de l'entreprise. (Farah, 2018)

2.2.1. Présentation de MEHARI

Tableau 1 : Présentation de MEHRI.

Lettre	Signification
M	Management (Gouvernance) : Cet élément met l'accent sur l'importance d'une culture et d'une structure de gouvernance solides en matière dans le domaine de la gestion des risques.
E	Évaluation : Cet élément met l'accent sur l'importance de l'identification et l'évaluation des risques : Cet aspect met l'accent sur
H	Humain : Cet aspect souligne l'importance de l'élément humain dans la gestion des risques.
A	Analyse : Ce composant souligne l'importance d'une méthode systématique dans l'analyse des risques
R	Réduction : Cet aspect se focalise sur l'élaboration et la mise en pratique de stratégies de gestion des risques.
I	Amélioration : Cet aspect met en avant la nécessité d'améliorer constamment le processus de gestion des risques.

Source : De la part de l'étudiante.

MEHARI, conçue et maintenue en France par **le CLUSIF depuis 1995**, est une méthode complète pour apprécier et administrer les risques associés à l'information, à son traitement et aux ressources qui y sont liées. MEHARI, disponible en français et anglais, est le produit des méthodes MARION et MELISA qui ne sont plus en activité depuis plusieurs années. MEHARI, en tant qu'instrument de protection des systèmes d'information, continue d'être largement adoptée, proposant une diversité d'approches pour gérer le risque au sein des structures organisationnelles.

MÉHARI dispose de trois bases de données de connaissances :

- **Méhari-Expert :** version conçue pour les grandes ou très grandes entreprises qui requiert une solide maîtrise de la méthode.
- **Méhari-Standard :** version destinée aux entreprises de taille moyenne ou grande, offrant davantage d'outils de gestion et un accès facilité.
- **Méhari-ManagerBC :** version dédiée à l'analyse spécifique d'activités ou de projets.

Créé en **1984**, le CLUSIF est une organisation française qui rassemble des sociétés et des collectivités. Son objectif principal est de traiter et de partager des informations concernant différents aspects de la sécurité de l'information tels que la gestion des risques, les politiques de sécurité et la cybercriminalité. Le site web du CLUSIF fournit un accès aux résultats de ses travaux, y compris la méthodologie MEHARI.

2.2.2. Objectifs

MEHARI a pour objectif principal de proposer une méthode exhaustive d'évaluation et de gestion des risques, en mettant l'accent sur le domaine de la sécurité des informations, tout en fournissant tous les instruments et ressources nécessaires à son application. Outre cet objectif principal, trois autres objectifs supplémentaires s'incluent :

- Il ne s'agit pas seulement de repérer les situations à risque et d'évaluer leur gravité, mais aussi de mettre en lumière les actions visant à réduire ces risques à un niveau acceptable.
- Permettre une étude directe et sur mesure des situations à risque grâce à l'élaboration de scénarios précis.
- Proposer un éventail exhaustif d'instruments adaptés à la gestion de la sécurité à court, moyen et long terme, indépendamment du degré de maturité de l'organisation concernant la sécurité et des types d'initiatives prévues.

2.2.3. Principe

2.2.3.1. Principe fondamental de MEHARI : Maîtrise totale du risque

Les composantes de MEHARI se basent sur un principe fondamental : ne jamais sous-estimer un risque. Cela se manifeste par deux principes de base :

- **Considérez toujours les scénarios les plus extrêmes possibles :** Il s'agit d'anticiper les conséquences les plus néfastes qui pourraient découler d'un risque donné, afin de mieux se préparer et d'adopter des mesures adéquates.
- **Prenez uniquement en compte les effets « contrôlés » des dispositifs de sécurité :** MEHARI se concentre sur l'évaluation pragmatique de l'efficacité des dispositifs de sécurité. On tient compte uniquement des impacts confirmés et quantifiables de ces actions, assurant ainsi une gestion des risques pragmatique et digne de confiance.

2.2.3.2. Un partenaire de confiance pour la sécurité de l'information

MEHARI propose un ensemble d'outils et de ressources précieux pour accompagner les organisations à gérer et protéger leurs informations. Ce cadre méthodologique exhaustif offre :

- **Une analyse approfondie des enjeux critiques :** MEHARI facilite l'identification et la compréhension des informations les plus critiques pour l'organisation, dans le but de hiérarchiser les mesures de protection.
- **Une analyse des vulnérabilités :** MEHARI assiste l'entreprise dans la détection et l'analyse des vulnérabilités potentielles de son système d'information, facilitant ainsi une prévention ciblée des risques.

- **Des stratégies efficaces pour atténuer la gravité des risques :** MEHARI offre des remèdes tangibles pour atténuer les effets potentiellement nuisibles des incidents de sécurité, réduisant par conséquent les préjudices infligés à l'entité.
- **Un pilotage éclairé de la sécurité de l'information :** MEHARI propose une gouvernance structurée pour la gestion des risques d'information, favorisant des décisions réfléchies et uniformes en ce qui concerne la sécurité de l'information.

2.2.3.3. Adaptabilité et flexibilité : Les avantages de MEHARI

Les modèles de risque MEHARI peuvent être modifiés pour répondre aux exigences particulières de chaque organisation, avec une personnalisation possible selon les directives stratégiques et les politiques de sécurité actuelles. Cette souplesse favorise la formulation de stratégies appropriées et simplifie le processus décisionnel efficace en termes de protection des informations.

2.2.3.4. Modèle de risque MEHARI : Une démarche à deux dimensions

- **Le modèle de risque qualitatif**

Cette méthode permet d'identifier les divers éléments d'un risque et les paramètres qui affectent son degré de sévérité. Elle propose une analyse détaillée des défis et encourage une appréciation exacte des dangers. (CLUSIF, 2010)

MEHARI suit une démarche systématique pour caractériser chaque risque en le présentant comme un scénario détaillé comprenant plusieurs composantes essentielles. Cette désagrégation facilite un examen détaillé et complet de chaque risque.

Pour assurer une identification des situations à risque standardisée et complète, MEHARI établit des typologies particulières. Ces classifications fournissent un cadre pour l'identification des risques, facilitant par conséquent une analyse minutieuse et structurée.

Ces mécanismes d'action, aussi connus sous le nom de « Facteurs de réduction du risque », se classifient en quatre grandes catégories :

- **Dissuasion :** Cette stratégie cherche à réduire la possibilité qu'un individu malintentionné prenne l'initiative de provoquer le risque, en décourageant son passage à l'acte par des actions adéquates.

- **Prévention :** Cette approche vise à rendre le risque plus difficile, voire improbable, en instaurant des dispositions qui empêchent la survenue de l'événement déclencheur.

- **Confinement :** Lorsque le risque se présente, l'objectif de confinement est de restreindre l'ampleur des dommages directs en appliquant des mesures de protection et de réduction des dégâts.

- **Palliation :** Cette méthode entre en jeu une fois le risque identifié et cherche à atténuer les effets indirects des dégâts infligés. Elle sert à minimiser l'effet global du risque sur l'entité.

➢ **Le modèle de risque quantitatif**

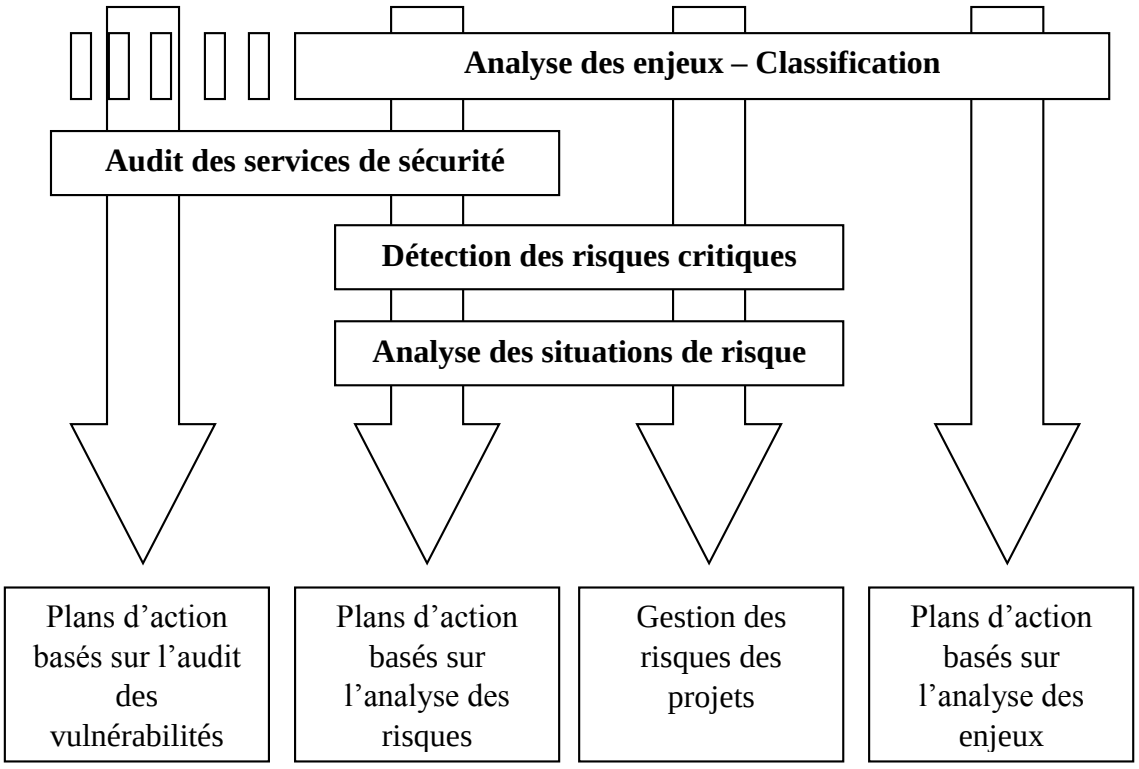
L'aspect « quantitatif » du modèle de risque MEHARI offre une composante quantitative fondamentale pour l'évaluation des risques, donnant aux entités la possibilité de classer leurs mesures préventives et d'estimer l'efficience de leurs plans de sécurité (CLUSIF, 2010)
Il comprend trois composantes principales :

- **Quantification des services de sécurité** : Ce processus consiste à déterminer et à quantifier l'efficacité des services de sécurité déployés pour faire face aux risques identifiés. Ceci permet d'évaluer leur véritable effet sur la diminution des risques.
- **Évaluation quantitative des facteurs de réduction de risque :** Pour chaque situation de risque examinée, MEHARI offre une estimation numérique des éléments de réduction du risque identifiés avant. Cette évaluation rend possible l'estimation exacte de l'influence de chaque élément sur la diminution du risque total.
- **Évaluation numérique de la gravité des risques :** En considérant les impacts cumulés des facteurs de minimisation du risque, MEHARI nous permet d'atteindre une évaluation numérique de la gravité de chaque risque. Cette méthode basée sur des données quantitatives fournit une appréciation précise et neutre du niveau de risque résiduel, ce qui facilite une prise de décision informée concernant la gestion des risques.

2.2.4. Processus

La méthode MEHARI est un outil pour le management des risques informatiques, comprend plusieurs phases distinctes, chacune ayant un rôle déterminant dans la détection, l'appréciation et la réduction des dangers éventuels.

Figure 4 : Représente le processus de la méthode MEHARI.



Source : (CLUSIF, 2010)

2.2.4.1. Analyse des enjeux: Poser les bases de la protection

La première phase de la méthode MEHARI consiste à examiner les enjeux. Elle a pour objectif de repérer les actifs essentiels de l'entité, qu'il s'agisse d'informations confidentielles, de systèmes informatiques ou d'infrastructures matérielles.

Cette phase essentielle consiste à établir la zone de protection et à hiérarchiser les initiatives de sécurité selon l'importance et le caractère critique des actifs identifiés.

L'examen des problématiques produit des plans d'action préliminaires qui constituent le fondement pour les phases suivantes. Ces stratégies pourraient comporter des actions préventives immédiates, comme l'instauration de sauvegardes fréquentes ou l'éducation des employés en matière de bonnes pratiques de sécurité.

2.2.4.2. Audit des services de sécurité : Évaluer les défenses existantes

L'évaluation des services de sécurité représente la seconde phase de la procédure MEHARI. Cela implique une analyse approfondie des mesures de sécurité actuellement instaurées au sein de l'entité. Cela englobe l'évaluation des pares-feux, des systèmes de détection d'intrusion, des contrôles d'accès ainsi que d'autres dispositifs de protection.

- **Résultat :** Plans d'action basés sur l'audit des vulnérabilités

L'évaluation des services de sécurité révèle les lacunes de sécurité actuelles et permet d'établir un inventaire détaillé des vulnérabilités possibles.

2.2.4.3. Détection des risques critiques : Identifier les menaces potentielles

La troisième phase de la démarche MEHARI se focalise sur l'identification des risques majeurs. Cette phase nécessite une étude détaillée des menaces internes et externes qui pèsent sur l'entité. Cela comprend l'évaluation des dangers associés aux programmes malveillants, aux attaques par déni de service, aux intrusions matérielles ainsi qu'à d'autres menaces éventuelles.

- **Résultat** : Analyse des situations de risque

L'examen des contextes de risque permet de repérer les situations spécifiques où une vulnérabilité pourrait être mise à profit par une menace. Cette évaluation détermine le degré de risque auquel l'organisation est exposée et facilite la hiérarchisation des mesures d'atténuation.

- **Plans d'action basés sur l'audit des vulnérabilités :** Cette phase implique la formulation de plans d'action ciblés afin de traiter les vulnérabilités mises en évidence lors de l'audit des services de sécurité. Cela peut englober des réparations de logiciels, des actualisations de sécurité ou des perfectionnements de procédures.
- **Plans d'action basés sur l'analyse des risques**

De façon analogue, cette phase nécessite l'élaboration de stratégies d'intervention pour faire face aux dangers repérés lors de l'évaluation des situations à risque. Ces stratégies peuvent se concentrer sur la prévention, l'atténuation ou la réaction face aux incidents de sécurité.

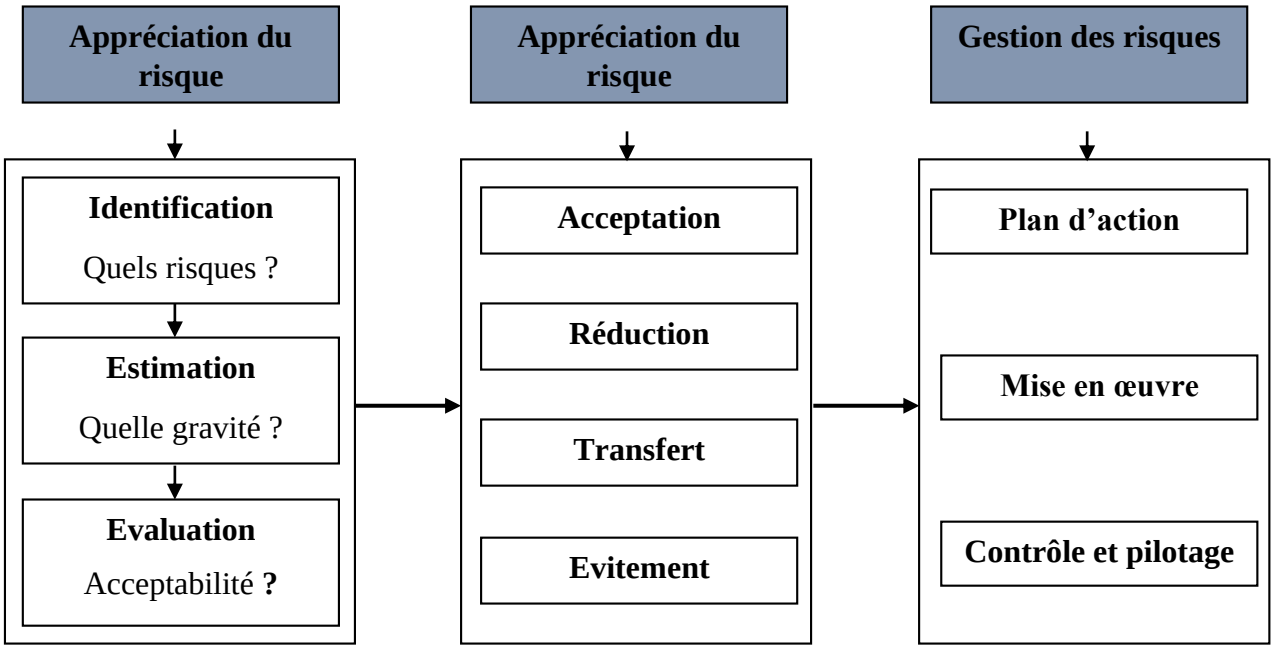
- **Gestion des risques des projets :** Cette composante vise à incorporer la gestion des risques de sécurité dans la planification et la mise en œuvre des projets de l'entité. Cela assure que les risques éventuels sont identifiés dès la phase initiale et gérés de façon adéquate tout au long du cycle de vie du projet.

- **Plans d'action basés sur l'analyse des enjeux :** Cette étape consiste à élaborer des stratégies concrètes pour traiter les problèmes de sécurité précédemment identifiés. Ces stratégies peuvent englober des actions de sécurité additionnelles, des sessions de

formation pour les employés ou encore des investissements dans des technologies sécuritaires récentes.

2.2.5. Méthodologie

Figure 5 : La méthodologie de la méthode MEHARI.



Source : Adapté de (CLUSIF, 2010)

2.2.5.1. Appréciation des risques

a) - Identification des risques : Cette première étape implique l'identification des risques potentiels susceptibles de compromettre un système d'information. Cela nécessite de collecter des informations issues de différentes sources, comme par exemple :

- **Sources internes :** Documentation du système, comptes rendus d'incidents, discussions avec le personnel et évaluations des faiblesses.
- **Sources extérieures :** Rapports sectoriels, articles de journaux et fil d'informations sur les menaces.

➢ **Les éléments distinctifs d'un risque**

- **L'actif :** C'est le composant du système d'information susceptible d'être affecté par le risque.

- **La vulnérabilité intrinsèque :** C'est une faiblesse propre à l'actif qui pourrait être mise à profit par une menace.
- **Le danger :** C'est un événement ou une circonstance susceptible de provoquer des dommages.
- **Le scénario de risque :** C'est une représentation précise du risque qui englobe tous les aspects caractéristiques évoqués précédemment.

➢ **Le processus de détection des risques MEHARI inclut les phases suivantes**

a- Conception de la liste des composantes caractéristiques des risques : Cette tâche consiste à déterminer les différentes catégories de composants caractéristiques des risques, comme l'actif, le niveau de criticité, les sortes de vulnérabilités, … etc.

b- Conception de l'inventaire potentiel des risques : L'objectif est d'énumérer toutes les combinaisons potentielles d'éléments caractéristiques liés aux risques.

c- Élaboration d'une base de données des risques standards : L'objectif est de constituer un répertoire qui inclut des descriptions des risques standardisés.

d- Choix des risques à considérer : Il est question de choisir les risques qui sont significatifs pour l'entreprise et qui sont soumis à la gestion des risques. (CLUSIF, 2010)

b) - Estimation de la probabilité et de l'impact des risques

➢ **Paramètres pour l'évaluation des risques**

La méthode MEHARI se fonde sur deux éléments essentiels pour apprécier le risque :

- **Potentialité :** La chance ou la probabilité qu'un certain risque se réalise. Elle illustre la possibilité que la menace devienne réalité.
- **Impact :** La sévérité des possibles répercussions si le danger se concrétise. Elle illustre l'étendue des dégâts que le risque pourrait infliger à l'entité.

➢ **Échelles de potentiel et d'impact :** MEHARI offre des échelles standardisées en quatre étapes pour la potentialité et l'impact, facilitant une évaluation cohérente et comparative des risques. Ces échelles considèrent divers éléments comme le type de menace, la susceptibilité des systèmes d'information et les compétences des intervenants malintentionnés.

- **Éléments qui influencent la potentialité intrinsèque :** L'impact intrinsèque d'un risque est aussi tributaire de divers éléments :

- **Importance des actifs informatiques :** La sévérité potentielle des répercussions est déterminée par la criticité des données et des systèmes d'information face à la menace.

- **Importance des processus d'affaires :** L'effet potentiel sur les opérations commerciales et la continuité des activités est un élément clé à considérer.

- **Risques financiers éventuels :** Il faut tenir compte des pertes financières directes et indirectes qui pourraient survenir si le risque se concrétise.

- **Atteinte à la réputation :** On ne doit pas sous-estimer les impacts néfastes sur l'image et la crédibilité de l'entité.

- **Effet des mesures de sécurité** Les mesures de sécurité sont cruciales pour minimiser les risques en agissant sur la probabilité et les conséquences.

- **Éléments diminuant la potentialité**

- **Mesures cumulées :**

Éviter l'occurrence de l'événement, par exemple en mettant en place des obstacles matériels ou des contrôles d'entrée.

- **Actions de dissuasion :**

Éviter que les menaces ne passent à l'acte, par exemple en affichant une présence sécuritair e notable ou en instaurant des politiques de dissuasion.

- **Actions préventives :**

Empêcher la réussite d'une attaque grâce à des dispositifs tels que le cryptage, les systèmes de détection d'intrusion ou encore les pares-feux.

- **Éléments réducteurs de l'impact**

- **Actions cumulatives :** Minimise les effets directs d'une attaque, par le biais de plans de reprise des activités suite à une catastrophe ou de procédures de sauvegarde.

- **Mesures d'isolement :** Réduire la diffusion des dégâts, par exemple en segmentant les données ou en divisant le réseau.

- **Stratégies d'atténuation :** Réduire les impacts indirects, tels que les plans de continuité des opérations ou les stratégies de gestion de la réputation.
- **Processus d'évaluation des risques :** Incarne deux étapes distinctes : stratégique et opérationnelle.

a - Développement des éléments de référence :

- Établissement des échelles d'impact, de potentiel et des niveaux pour les facteurs de réduction des risques.
- L'objectif est d'établir une hiérarchie entre les niveaux de conséquences, de probabilité et d'efficacité des mesures de sécurité.

b - Évaluation des risques :

- Évaluation de l'impact et du potentiel intrinsèques.
- Analyse des éléments pour diminuer les risques.

- Recherche des mesures de sécurité appropriées pour chaque situation à risque.

- Définition des conséquences des mesures et des niveaux associés.

- La détermination du degré de chaque facteur de réduction de risque se fait en se basant sur les niveaux maximaux obtenus grâce aux mesures appropriées.

- **Évaluation de l'impact et du potentiel résiduel des risques**

- Fondée sur les évaluations internes et les éléments de minimisation des risques.
- Emploi de matrices décisionnelles pour assurer la reproductibilité des jugements, selon le type de situation à risque. **(CLUSIF, 2010)**

c)- Évaluation de l'acceptabilité des risques

L'évaluation de l'acceptabilité de chaque risque constitue la phase finale dans l'estimation des risques. Cela implique de déterminer si le risque est acceptable ou s'il nécessite une intervention quelconque.

Lors de l'évaluation de l'acceptabilité d'un risque, plusieurs éléments doivent être considérés, comme par exemple :

- La conséquence financière éventuelle du risque.

- L'influence éventuelle sur la réputation de l'établissement.
- La mise à disposition de mesures pour réduire le risque.
- Le seuil d'acceptation du risque par l'organisation.

La méthode MEHARI, offrant une approche exhaustive pour l'évaluation et la gestion des risques, regroupe ceux-ci en trois catégories selon leur sévérité générale :

- **Risques intolérables (Niveau de gravité 4)**

Ces risques représentent une menace inacceptable pour l'entité et requièrent une intervention immédiate. Ils réclament des actions d'atténuation immédiates pour éviter ou réduire les éventuels préjudices.

- **Risques inadmissibles (Niveau de gravité 3)**

Ces risques sont jugés comme des menaces majeures qu'il faut supprimer ou atténuer dans un laps de temps déterminé. Ils nécessitent une attention immédiate et des stratégies de gestion des risques priorisées pour les réduire à un niveau acceptable.

- **Risques admissibles (Niveaux de gravité 1 et 2)**

Ces risques sont considérés comme maîtrisables et peuvent être tolérés selon la tolérance au risque de l'organisation. Cependant, une supervision constante et des actions d'atténuation éventuelles demeurent indispensables pour s'assurer qu'ils se maintiennent dans des limites tolérables.

➢ **Évaluer la sévérité du risque :** MEHARI emploie une procédure en deux phases pour classer un risque dans l'une de ces catégories :

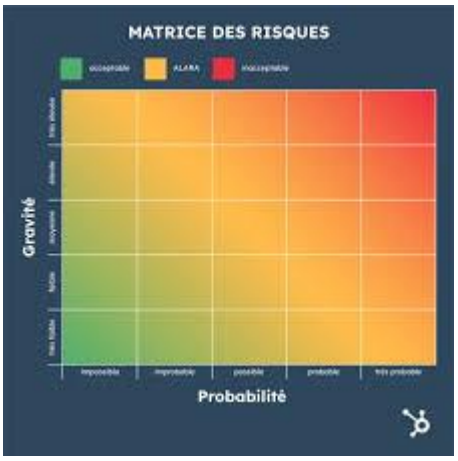
a- Évaluer la probabilité du risque : Estimer la probabilité de survenue du risque, en considérant des éléments comme les données passées, les orientations sectorielles et les appréciations de vulnérabilité. Accorder une note de probabilité allant de 1 (très basse) à 5 (très haute).

b- Matrice d'évaluation des risques : Évaluer les impacts possibles de la concrétisation du risque, en considérant des éléments comme les pertes économiques, les dommages à l'image de marque et les troubles dans le fonctionnement opérationnel. Accorder une note d'impact allant de 1 (très bas) à 5 (très haut).

➢ **Matrice d'évaluation des risques**

MEHARI se sert d'une matrice de gravité des risques qui fusionne les indices de probabilité et d'impact afin d'évaluer le degré global de sévérité du risque. (CLUSIF, 2010)

Figure 6 : Matrice gravité impact probabilité.



2.2.5.2. Traitement des risques

Après l'identification et l'évaluation des risques, la phase suivante est de déterminer la manière de les gérer. Cela consiste à choisir la stratégie de gestion la plus adaptée à chaque risque et à élaborer un plan pour sa mise en pratique.

Pour ce faire, MEHARI suggère quatre approches pour gérer les risques détectés :

a -Accepter : La décision d'accepter un risque est généralement prise lorsque celui-ci est considéré comme acceptable ou lorsqu'il n'y a pas d'alternatives de mitigation viables ou avantageuses. Le risque est accepté dans le cas où :

- Dans la « grille d'acceptabilité des risques », le risque a été jugé comme acceptable.
- Dans le cadre de considérations économiques (ou autres), il a été déterminé qu'il n'était pas possible de trouver une solution.

b – Réduire : Sélectionner des services de sécurité à partir d'une "base de connaissances" implique : Identifier chaque service avec sa finalité ou son objectif spécifique.

- Détailler les mécanismes techniques et organisationnels nécessaires à sa mise en œuvre efficace.
- Évaluer chaque service selon un niveau de qualité prédéfini, afin de :

- Fournir une évaluation globale lors de la combinaison de plusieurs services.

- S'assurer que le risque est réduit à un niveau de gravité acceptable.

Quand minimiser un risque ?

- Le danger est intolérable, mais il peut être réduit grâce à des actions rentables.
- Des solutions d'atténuation efficaces sont disponibles.
- Les bénéfices potentiels de l'atténuation surpassent les coûts.

c- Transférer : Le transfert de risque implique le transfert de la responsabilité financière d'un risque à une autre entité. Ceci peut être réalisé à travers une assurance, une externalisation ou d'autres arrangements contractuels.

À quel moment faut-il transférer un risque ?

- Le risque est tellement élevé que l'organisation ne peut pas le prendre en charge de façon indépendante.
- Il y a une tierce partie prête et en mesure d'assumer le risque
- Le coût de la cession du risque est moins élevé que le coût potentiel lié à ce risque.

d – Éviter : L'évitement des risques implique la suppression totale du risque en modifiant le plan d'action ou l'activité commerciale. C'est une approche potentiellement très efficace pour gérer les risques, mais elle peut également représenter l'option la plus complexe et onéreuse.

Quand faut-il éviter un risque ?

- Le risque est inadmissible et ne peut être réduit ou délégué.
- Les bénéfices compensent les coûts d'évitement.
- On dispose d'une alternative distincte et praticable à l'activité à risque.

d)- Gestion des risques : L'intervention de la gestion des risques se produit après que des décisions ont été prises en ce qui concerne le traitement des risques. Elle comprend tous les processus requis pour appliquer ces décisions, surveiller leurs impacts et les perfectionner si besoin. Le processus de création des plans d'action inclut plusieurs phases :

- La mise en œuvre des services de sécurité a été effectuée, chaque service ayant un but précis en matière de qualité.

- Implémentation de mesures structurelles dans le but de diminuer l'exposition à divers risques.
- Mise en place de dispositions organisationnelles pour prévenir certaines menaces.

a -Sélection et optimisation des objectifs prioritaires : Pour établir les priorités, il est crucial de considérer divers éléments, dont :

- Les niveaux de gravité des risques que les actions prioritaires permettront de diminuer. Il faut prioriser le traitement des risques les plus importants.
- Le volume de risques gérés sur-le-champ et ceux dont la gestion sera reportée.
- La célérité avec laquelle les premiers résultats pourront être constatés.
- L'effet de ces décisions sur la prise de conscience du personnel, entre autres.

b -Sélection des solutions : La sélection des solutions est déterminée par des équipes d'experts comme la Direction des Systèmes d'Information (DSI), les gestionnaires de réseaux, les responsables de la sécurité physique, les RSSI, et ainsi de suite. Ces solutions sont rassemblées dans un guide de référence des services de sécurité, qui inclut :

- La finalité de chaque service.
- Les résultats escomptés suite à l'implémentation du service.
- Une explication des processus liés à chaque service, qu'ils soient de nature technique ou organisationnelle.
- Les normes utilisées pour juger la qualité de chaque service.

MEHARI offre un guide de référence en matière de services de sécurité, et pour assurer leur efficacité, il est nécessaire de procéder à des vérifications :

- Au premier stade, pour s'assurer que les mécanismes et solutions de sécurité envisagés sont en adéquation avec les standards de qualité de service sélectionnés lors du processus d'évaluation des risques.
- Au niveau deux, pour superviser la mise en application effective de ces solutions. (CLUSIF, 2010)

CHAPITRE ⅠⅠ: CADRE METHODOLOGIQUE ET CONTEXTE ORGANISATIONNEL

1.Cadre Méthodologique

1.1 Approche épistémologique

Toute recherche en sciences de gestion repose sur une posture épistémologique explicite, qui oriente le choix des méthodes et encadre l'interprétation des résultats (Guba, 1994). Dans cette étude, dont l'objectif est d'évaluer un modèle de gestion des risques de cybersécurité au sein d'un cadre de gouvernance IT, nous adoptons une posture constructiviste. Le constructivisme postule que la réalité se construit socialement à travers les interactions et les interprétations des acteurs, plutôt que d'exister comme une réalité objective et déterminée (Berger, 1996). Cette orientation est particulièrement adaptée à notre étude de cas chez NAFTAL, où les pratiques de cybersécurité et les dispositifs de gouvernance sont sans cesse façonnés par les processus organisationnels internes et les technologies émergentes.

1.2 Approche méthodologique

Pour répondre à notre question de recherche, nous adoptons une démarche qualitative, privilégiant l'étude des représentations et des mécanismes plutôt que la vérification d'hypothèses formelles (Creswell, 2013). Cette approche nous permet de nous appuyer sur la richesse des perceptions des parties prenantes tout en comprenant la complexité des pratiques de gestion des risques de cybersécurité au sein de NAFTAL.

Les principales méthodes utilisées sont, les entretiens semi directive, l'observation, analyse documentaire.

Ces approches complémentaires permettent une triangulation des données (Denzin, 1978), renforçant ainsi la validité et la crédibilité des résultats en ancrant notre cadre conceptuel dans la réalité organisationnelle observée.

1.3. Méthode de collecte de données

La collecte de données constitue une phase essentielle de cette recherche, visant à évaluer un système de gestion des risques de cybersécurité dans le cadre d'une gouvernance IT. Ce travail s'inscrit dans le cadre d'un mémoire de fin d'études à l'École Nationale Supérieure de Management (ENSM), associé à un stage pratique au sein de NAFTAL. Afin de garantir la pertinence, la validité et la triangulation des résultats (Denzin, 1978), trois méthodes convergentes de collecte de données ont été mobilisées : recherche documentaire, observation de terrain et entretiens semi-structurés (Creswell, 2013)

1.3.1. Recherche documentaire

La première activité a consisté en une recherche documentaire approfondie. Celle-ci a couvert :

- La littérature académique (ouvrages spécialisés, articles scientifiques, rapports d'experts) permettant de cadrer théoriquement notre sujet (Boiral, 2007) ;
- Les référentiels et normes internationaux en cybersécurité et en gouvernance IT (ISO/IEC 27001, NIST Cybersecurity Framework, COBIT 2019), reconnus pour structurer les bonnes pratiques ((ISACA, 2021) ; NIST, 2018).
- Des documents internes à NAFTAL (plans de sécurité, politiques internes, procédures, rapports d'audit), obtenus durant le stage.

Cette étape a permis de construire le cadre conceptuel de l'étude, d'identifier les meilleures pratiques en cybersécurité et de comprendre les enjeux spécifiques liés à la gouvernance IT (Von Solms, 2013).

1.3.2. Observation de terrain

Dans le cadre du stage au sein du département informatique de NAFTAL, nous avons mené une observation participante (Merriam, 1998), permettant une immersion dans les dynamiques organisationnelles. Cette méthode nous a offert un accès direct aux pratiques effectives, incluant :

- La gestion opérationnelle des risques ;
- L'usage des outils de cybersécurité ;
- Les flux d'information et les dispositifs de contrôle d'accès ;
- Les procédures de réponse aux incidents et la gestion des responsabilités.

Cette observation a contribué à évaluer le niveau de maturité de la culture de sécurité, tout en identifiant les écarts entre les procédures formelles et leur mise en œuvre effective (Weick, 2007)

1.3.3. Entretiens semi-structurés

Pour approfondir notre compréhension des pratiques de gouvernance IT et de gestion des risques cyber chez NAFTAL, nous avons mené des entretiens semi-structurés **(**Kvale, 2009) auprès d'acteurs clés :

- Le Responsable de la Sécurité des Systèmes d'Information (RSSI) ;
- Des membres de la DSI ;
- Des ingénieures de la sécurité des systèmes d'information.

Un guide d'entretien élaboré à partir de notre question de recherche portait sur les thèmes suivants: Stratégie de gouvernance IT à NAFTAL; Intégration de la cybersécurité dans la gouvernance IT; Identification et gestion des risques en cybersécurité; Mesures de protection des systèmes d'information ; Sensibilisation des employés de la DSI aux risques cyber; Méthodes d'évaluation des risques de cybersécurité; Outils et méthodologies utilisés (dont MEHARI); Difficultés rencontrées dans l'évaluation des risques; Rôle de la direction générale dans la gouvernance IT et la cybersécurité.

Chaque entretien, d'une durée de 45 à 60 minutes, a été enregistré avec le consentement des participants, puis intégralement transcrit pour permettre une analyse thématique rigoureuse (Braun, 2006).

Tableau 2 : liste des interviewés.

Interviewé	Profession	Lieu de l'entretien	Durée de l'entretien	Méthode de l'entretien
Interviewé 1	RSSI	Le bureau	1 h	Face à face
Interviewé 2	CHEF DE PROJET SECURITY SI	Le bureau	45 min	Face à face
Interviewé 3	CHEF DE DEPARTEMENT SOC	Le bureau	1 h	Face à face
Interviewé 4	INGENIEUR SECURITY SYSTEM	Le bureau	45 min	Face à face
Interviewé 5	CADRE INFORMATIQUE NIV3	Le bureau	45 min	Face à face

Source : élaboré par mes soins.

1.4. Le guide d'entretien

Notre guide d'entretien, destiné aux responsables de la Direction des Systèmes d'Information (DSI) de NAFTAL, est structuré de la manière suivante :

• Thème 1 : Gouvernance IT

Ce thème explore la stratégie globale de gouvernance des technologies de l'information à NAFTAL. Il s'agit de comprendre comment elle est alignée avec les objectifs de l'entreprise, quels sont ses composants clés, ainsi que le rôle joué par la direction générale dans sa mise en œuvre, en particulier vis-à-vis des risques cyber.

• Thème 2 : Gestion des risques et cybersécurité

Cette section porte sur les pratiques actuelles de gestion des risques informatiques à NAFTAL. Les questions visent à identifier les types de risques les plus fréquents, les mesures de protection adoptées, ainsi que les dispositifs de sensibilisation du personnel aux enjeux de cybersécurité.

• Thème 3 : Méthodes d'évaluation des risques

Ce thème s'intéresse aux outils, méthodes et indicateurs utilisés pour évaluer les risques de cybersécurité au sein de NAFTAL. Il aborde la façon dont les résultats de ces évaluations sont intégrés dans les processus de gouvernance et d'amélioration continue, ainsi que les éventuelles difficultés rencontrées dans leur mise en œuvre.

• Thème 4 : Pertinence de la méthode MEHARI

La dernière section est consacrée à l'utilisation potentielle ou réelle de la méthode MEHARI dans l'évaluation des risques chez NAFTAL. Les questions portent sur la connaissance de la méthode, son efficacité perçue, ses avantages et limites, et sa pertinence éventuelle pour une intégration durable dans la stratégie de gouvernance IT de l'entreprise.

• Clôture

L'entretien se termine par des remerciements adressés aux participants, ainsi qu'une question ouverte permettant aux répondants d'ajouter tout commentaire ou remarque jugée utile à la compréhension du sujet.

2. Contexte organisationnelle

Figure 7 : Logo de l'entreprise NAFTAL.

NAFTAL**,** Une entreprise fondée en 1982 par SONATRACH, elle est spécialisée dans la distribution et la commercialisation de produits pétroliers et dérivés sur l'ensemble du territoire national.

NAFTAL joue un rôle central dans l'approvisionnement en carburants, lubrifiants, gaz de pétrole liquéfié (GPL), bitumes et autres produits énergétiques indispensables à l'économie algérienne. Avec un réseau dense de stations-service et d'infrastructures logistiques (pipelines, citernes, dépôts, transport routier et ferroviaire), elle assure la continuité énergétique dans tous les coins du pays. Le siège social de l'entreprise est situé à Chéraga, Alger.

2.1. NAFTAL

2.1.1. Histoire et structure

Créée en 1981, NAFTAL (abréviation de *NAFTAlianes*) est le fruit de la réorganisation du secteur pétrolier algérien, dans un contexte où l'État cherchait à centraliser et rationaliser la distribution des produits pétroliers à l'échelle nationale. À l'origine, ses activités regroupaient plusieurs entités opérant indépendamment dans la commercialisation des carburants et des lubrifiants.

En 1987, NAFTAL devient une entreprise nationale autonome, tout en demeurant une filiale à 100 % du groupe SONATRACH, leader national de l'énergie. Ce rattachement lui confère un rôle stratégique dans le dispositif énergétique du pays.

En 1998, dans un souci de modernisation et d'adaptation au marché, NAFTAL adopte le statut de Société par Actions (SPA). Depuis, elle a connu une transformation significative :

- Développement d'un réseau national dense de stations-service ;
- Modernisation de ses infrastructures logistiques ;

- Diversification de ses produits et services (GPL, lubrifiants, bitumes, etc.).

Aujourd'hui, NAFTAL est l'unique distributeur national de produits pétroliers en Algérie et un acteur majeur de la souveraineté énergétique du pays, par son rôle dans l'approvisionnement, la sécurité énergétique et la transition vers des énergies plus propres comme le GPL carburant.

2.2. Direction Générale de NAFTAL

2.2.1. Siège et rôle stratégique

La Direction Générale de NAFTAL est située à Chéraga (Alger), plus précisément sur la Route des Dunes. Elle représente le centre névralgique décisionnel de l'entreprise. À ce titre, elle est responsable de :

- L'élaboration et le suivi de la stratégie nationale de distribution des produits pétroliers et gaziers ;
- La coordination des activités techniques, logistiques, commerciales et administratives sur l'ensemble du territoire national ;
- La supervision des projets d'innovation, de développement durable et de modernisation technologique.

2.2.2. Services offerts

NAFTAL propose une offre diversifiée de produits et de services couvrant les besoins énergétiques des particuliers, entreprises et institutions publiques. Parmi ses prestations principales, on trouve :

- Distribution de carburants : essence, gasoil, carburant diesel, etc.
- Commercialisation de gaz GPL : pour usage domestique et carburant (GPL-c).
- Vente de lubrifiants et bitumes : destinés aux secteurs automobiles, industriel et routier.
- Entretien et services automobiles : proposés dans les stations-service (vidange, lavage, pneus, etc.).
- Solutions logistiques : transport, stockage et distribution à l'échelle nationale.

2.2.3. Clientèle

La clientèle de NAFTAL est très variée, englobant :

- Les particuliers (à travers son réseau de stations-service) ;
- Les entreprises publiques et privées, notamment dans les secteurs :
  - Du transport et de la logistique ;
  - De l'industrie lourde et manufacturière ;
  - De la construction et travaux publics ;
  - Des administrations et collectivités locales.

NAFTAL s'inscrit donc dans une dynamique de service universel, avec des produits accessibles à toutes les catégories de clients sur tout le territoire.

2.2.4. Positionnement stratégique

Avec plus de 2 300 stations-service, des dépôts répartis dans toutes les régions, et un système logistique intégré, NAFTAL détient une position de monopole dans la distribution des produits pétroliers en Algérie.

Elle se distingue par :

- Une couverture géographique quasi totale du territoire national ;
- Un rôle essentiel dans la chaîne d'approvisionnement énergétique du pays ;
- Une capacité à répondre rapidement aux besoins de consommation en zones urbaines comme rurales.

En plus de son rôle économique, NAFTAL assume une responsabilité sociétale en accompagnant les politiques publiques de transition énergétique, notamment via la promotion du GPL carburant, jugé plus propre et moins coûteux.

2.2.5. Missions de la Direction Centrale des Systèmes d'Information (DCSI) et de ses structures rattachées

La **Direction Centrale des Systèmes d'Information (DCSI)** de NAFTAL joue un rôle stratégique dans la mise en œuvre de la politique numérique de l'entreprise. Elle est chargée de concevoir, déployer et sécuriser les systèmes d'information à l'échelle nationale, dans une logique de performance, d'intégration et de conformité.

Elle se compose de quatre directions et un département transversal, chacun ayant des missions spécifiques et complémentaires visant à garantir la gouvernance, la continuité et la sécurité des infrastructures informatiques et du patrimoine informationnel de l'entreprise.

a. Direction des Infrastructures

Cette direction est responsable de la conception et de la mise en œuvre de l'architecture technique du système d'information. Ses missions incluent :

- La définition de l'architecture des réseaux, serveurs et bases de données ;
- L'optimisation des infrastructures physiques et logiques pour garantir la performance et la fiabilité du SI.

b. Direction des Solutions Métiers

Elle a pour mission de développer des solutions applicatives adaptées aux besoins opérationnels des différentes entités de NAFTAL. Cela inclut :

- L'analyse fonctionnelle des besoins des utilisateurs ;
- La conception, le développement et l'intégration de solutions logicielles métier ;
- L'accompagnement des utilisateurs dans la prise en main des outils.

c. Direction des Opérations

Cette direction assure l'exploitation et la disponibilité des systèmes en production, notamment :

- Le bon fonctionnement des plateformes monétiques et décisionnelles ;
- La maintenance et la supervision des équipements informatiques des utilisateurs finaux ;
- La gestion des incidents techniques affectant les opérations quotidiennes.

d. Direction des Informations Documentaires

Elle est en charge de la gestion du patrimoine documentaire de l'entreprise. Ses responsabilités incluent :

- Le recensement des besoins en archivage, versement, élimination ou acquisition de documents (supports papier ou électroniques) ;

- L'élaboration de programmes annuels d'archivage, de suivi des inspections documentaires et de gestion des fonds documentaires internes ;
- Le déploiement de solutions d'archivage électronique sécurisé.

e. Département Sécurité & Conformité

Ce département transversal a une mission essentielle : assurer la sécurité, l'intégrité et la pérennité du système d'information de NAFTAL. Il s'occupe notamment de :

- La conception et le déploiement des politiques de sécurité informatique ;
- Le contrôle de conformité.
- Les normes internes et les réglementations en vigueur la mise en œuvre de plans de continuité et de reprise d'activité (PCA/PRA).

f. Missions globales de la DCSI

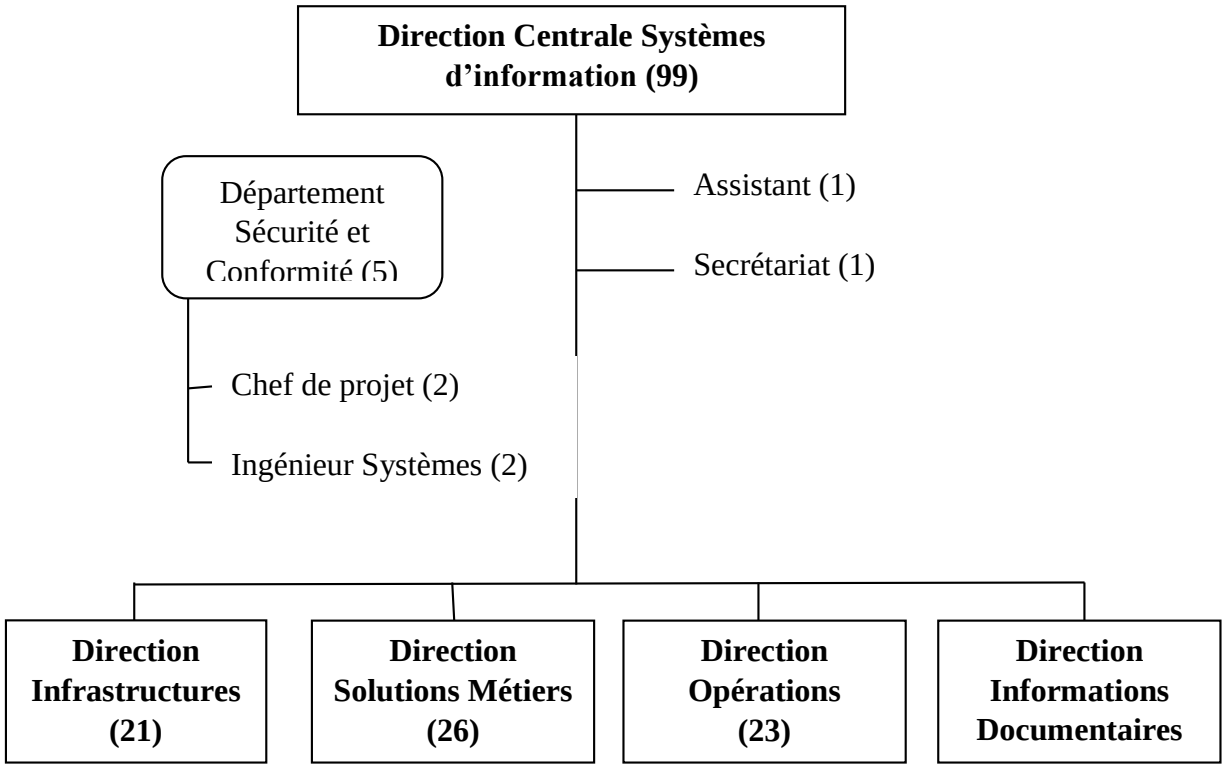
Outre les missions spécifiques de ses entités, la DCSI assume des fonctions transversales stratégiques qui s'inscrivent pleinement dans la gouvernance IT de NAFTAL :

- Modernisation des systèmes existants et migration vers des plateformes plus performantes ;
- Déploiement de progiciels de gestion intégrée (ERP) et d'outils d'aide à la décision ;
- Interconnexion de l'ensemble des structures via un réseau informatique étendu et sécurisé ;
- Mise en place de règles uniformes de gestion du réseau et supervision de leur application ;
- **Planification et rationalisation du parc informatique** ;
- Développement de **banques de données de gestion et documentaires** pour appuyer le pilotage stratégique ;
- **Supervision des projets SI** : de la conception à la formation, en passant par l'analyse, le déploiement et l'assistance ;
- **Mise en œuvre de solutions de cybersécurité** pour protéger les actifs numériques et les informations sensibles ;
- **Respect de la conformité logicielle** (licences, droits d'usage) ;

- **Renforcement des compétences** du personnel SI à travers des formations ciblées et un accompagnement dans l'évolution technologique.

Cette organisation démontre que NAFTAL place les systèmes d'information et la cybersécurité au cœur de sa stratégie de gouvernance IT, en dotant sa DCSI d'une structure complète, spécialisée et tournée vers la performance, la sécurité et l'innovation.

Figure 8 : Organigramme Direction Centrale Systèmes d'information (DCSI).



Source : Document interne NAFTAL.

2.2.6. Organigramme

NAFTAL S.p.a dispose d'une structure organisationnelle rigoureusement conçue pour piloter ses activités dans le secteur énergétique, articulée autour de trois piliers complémentaires : gouvernance stratégique, branches opérationnelles et fonctions support spécialisées.

a. Niveau Directionnel

Sous l'autorité du Président Directeur Général, l'organe décisionnel intègre :

- Un Secrétariat Général assurant la coordination transverse

- Des instances consultatives (Comité Exécutif, Comité de Direction)
- Un dispositif de conseil stratégique via les Conseillers

b. Pôles Opérationnels

Le Secrétariat Général supervise quatre divisions clés :

- La Branche Carburants (cœur de métier historique)
- La Branche Commercialisation (optimisation de la distribution)
- La Branche GPL (spécialisation gazière)
- Le Pôle Projets Internationaux (développement offshore)

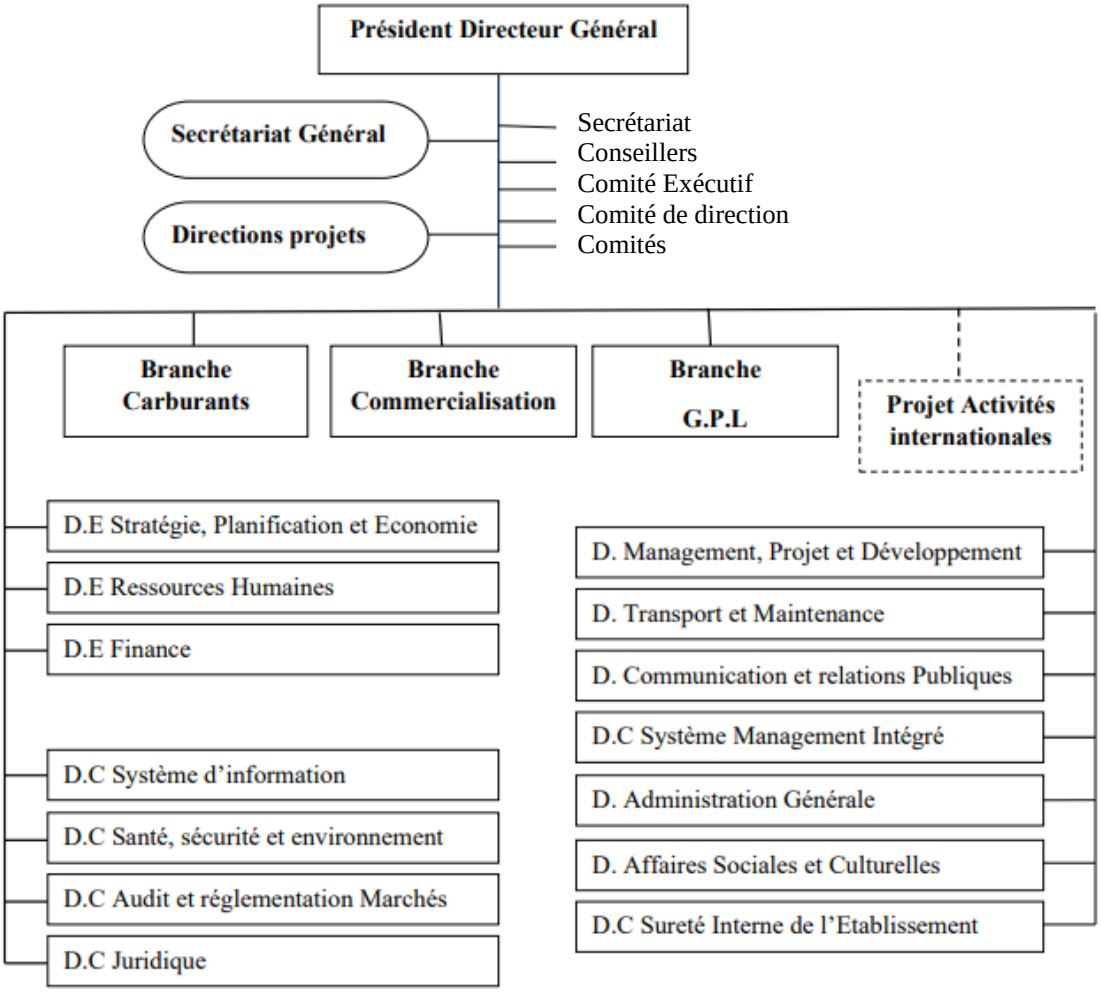
c. Directions Fonctionnelles

Huit départements experts soutiennent les opérations :

- Pilotage économique (Stratégie/Finances)
- Capital humain (RH/Affaires Sociales)
- Conformité (Audit/Juridique)
- Infrastructures (Transport/Systèmes d'Information)
- Management intégré (QHSE/Communication)

Cette architecture organisationnelle permet à NAFTAL d'allier réactivité opérationnelle et vision stratégique, tout en garantissant la conformité réglementaire et l'optimisation de ses processus clés. La présence de cellules dédiées aux activités internationales et à l'innovation reflète par ailleurs une volonté d'expansion et d'adaptation aux évolutions du marché énergétique.

Figure 9: Schéma de la macrostructure de NAFTAL S.p.a



Source : Document Interne - NAFTAL.

2.2.7. Hiérarchie de la Direction de la Sécurité des Systèmes d'Information (DSSI) – NAFTAL

La Direction de la Sécurité des Systèmes d'Information (DSSI), également désignée comme le RSSI (Responsable de la Sécurité des Systèmes d'Information) ou le CISO (Chief Information Security Officer), est directement rattachée à la Direction Générale de NAFTAL. Elle a pour responsabilité la mise en œuvre des politiques de cybersécurité, la gestion des risques informatiques et la conformité aux normes en vigueur.

➢ **Structure organisationnelle de la DSSI**

- **Direction Sécurité SI (RSSI / CISO)**

↳ Appuyée par un **secrétariat administratif**

- **Trois pôles fonctionnels principaux :**

a. Pôle SOC (Security Operations Center)

- Responsable SOC
- Chef de projet SOC
- Analyste sécurité
- Ingénieurs spécialisés

b. Pôle Projets Sécurité

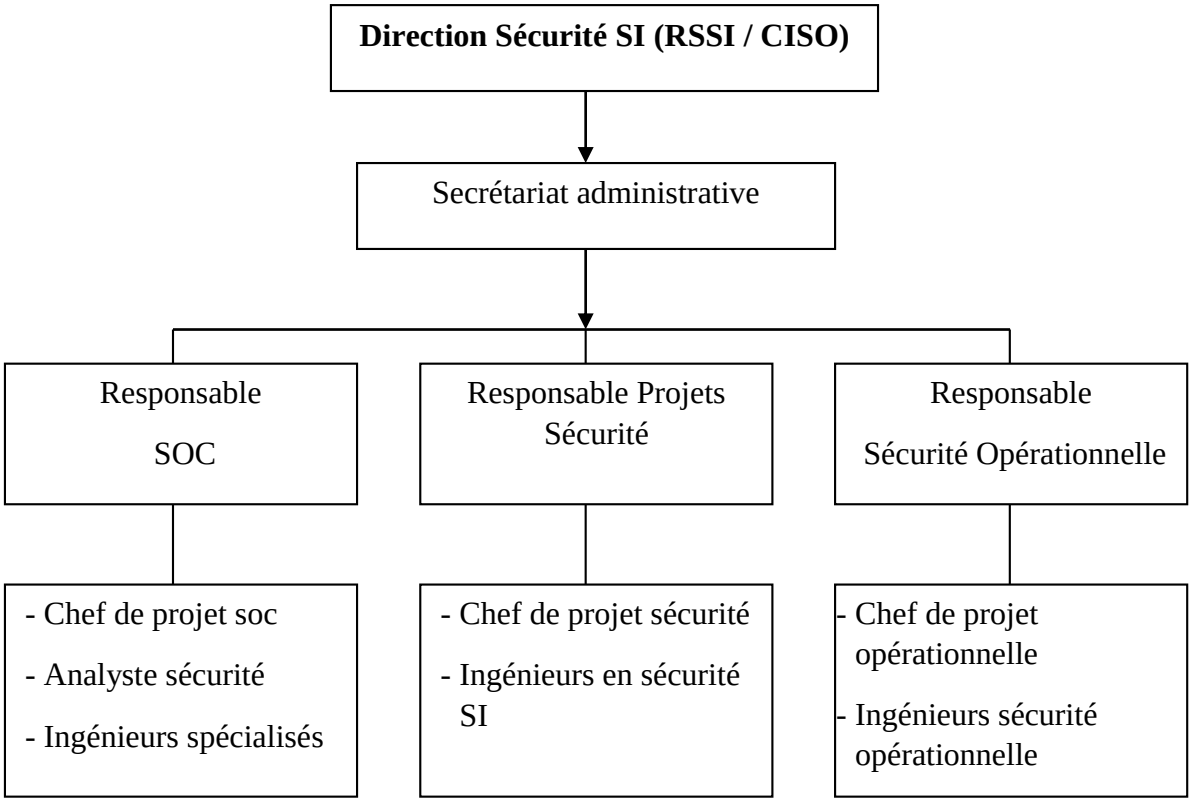
- Responsable des projets sécurité
- Chef de projet sécurité
- Ingénieurs en sécurité des SI

c. Pôle Sécurité Opérationnelle

- Responsable sécurité opérationnelle
- Chef de projet
- Ingénieurs sécurité opérationnelle

Cette organisation permet une gestion efficace et segmentée de la sécurité de l'information, avec une distinction claire entre la surveillance en temps réel (SOC), la conduite de projets sécuritaires, et l'exécution des actions de sécurité au quotidien.

Figure 10 : Organigramme fonctionnel de la (DSSI) de NAFTAL.



Source : Document interne – DSSI NAFTAL.

2.2.8. Analyse SWOT

Tableau 3 : Analyse SWOT – NAFTAL (Cybersécurité et Gouvernance IT)

Strengths	**Weaknesses**
• Système d'information structuré à l'échelle nationale	• Absence d'un cadre formel intégré pour la gouvernance, les risques et la conformité (GRC)
• Implication croissante de la direction dans les enjeux numériques	• Faible sensibilisation des employés à la cybersécurité
• Présence d'une DSI spécialisée	• Faible exploitation des méthodologies structurées (MEHARI, ISO 27005, etc.)
• Réseau d'agences interconnectées permettant la centralisation des données critiques	• Dépendance à certains systèmes informatiques anciens et peu flexibles
Opportunities	**Threats**
• Contexte favorable à la transformation numérique	• Évolution rapide et complexe des menaces cybernétiques
• Possibilité d'adopter des normes internationales (ISO 27001, 27005, etc.)	• Risque de non-conformité avec les réglementations nationales et internationales
• Potentiel de partenariats avec des experts en cybersécurité ou cabinets spécialisés	• Résistance interne au changement organisationnel
• Développement d'expertise interne en cybersécurité adaptée au contexte algérien	• Surface d'attaque élargie en raison de l'interconnexion avec des partenaires et tiers externes

Source : Élaboration personnelle à partir des entretiens réalisés chez NAFTAL et de l'analyse documentaire.

CHAPITRE ⅠⅠⅠ : RESULTAT ET DISSCUSION

Section 1 : Analyse des résultats

Afin de mieux comprendre l'état actuel de la gestion des risques liés à la cybersécurité chez NAFTAL, cette section présente et analyse les principaux résultats issus des données collectées. En s'appuyant sur les entretiens menés auprès des responsables de la DSI, les observations de terrain ainsi que les enseignements de la revue de littérature, cette analyse permet d'évaluer les pratiques existantes, d'identifier les forces et faiblesses du dispositif en place, et de mettre en évidence les écarts par rapport aux cadres de référence reconnus. Elle constitue ainsi une base essentielle pour formuler des recommandations adaptées dans la section suivante.

1. Étude de l'existant

Chez NAFTAL, la gestion des risques liés aux systèmes d'information constitue un enjeu stratégique, notamment dans un contexte marqué par la transformation numérique et l'augmentation des menaces cybernétiques. Pour y faire face, l'entreprise adopte une approche méthodologique structurée et conforme aux normes internationales, s'appuyant principalement sur la norme ISO/IEC 27005, dédiée à la gestion des risques liés à la sécurité de l'information.

L'ISO/IEC 27005 fournit un cadre normatif reconnu qui aide à identifier, évaluer, traiter et surveiller les risques pouvant affecter la confidentialité, l'intégrité et la disponibilité des actifs informationnels. Cette approche s'inscrit dans la logique d'un Système de Management de la Sécurité de l'Information (SMSI) conforme à la norme ISO/IEC 27001. En évaluant les menaces, les vulnérabilités, les impacts potentiels et les niveaux de risque résiduel, l'organisation est en mesure de formuler des plans de traitement adaptés, contribuant ainsi à la résilience organisationnelle et à la conformité réglementaire.

Cependant, bien que l'ISO/IEC 27005 constitue une base robuste et stratégique, la méthode MEHARI (Méthode Harmonisée d'Analyse des Risques) peut apporter une perspective complémentaire en se focalisant sur l'analyse opérationnelle et scénarisée des risques. MEHARI permet une évaluation plus fine et plus concrète des risques de sécurité, grâce à des outils décisionnels qui facilitent la priorisation des mesures correctives et l'identification des points de vulnérabilité.

L'utilisation conjointe de l'ISO/IEC 27005 et de MEHARI permettrait à NAFTAL de bénéficier d'une approche à la fois stratégique et opérationnelle, renforçant ainsi l'efficacité de sa gouvernance IT et de sa cybersécurité.

Tableau 4 : Tableau comparatif entre ISO/IEC 27005 et MEHARI.

Critères	ISO/IEC 27005	MEHARI
Objectif principal	Cadre de gestion des risques liés à la sécurité de l'information dans un SMSI.	Outil d'aide à la décision pour l'analyse opérationnelle des risques.
Portée	Large : tout type de risques (organisationnels, techniques, juridiques, etc.)	Ciblée : focalisée sur les risques liés aux systèmes d'information.
Méthodologie	Basée sur une approche continue de gestion des risques (identification, analyse, évaluation, traitement, acceptation, surveillance).	Approche détaillée par étapes : mesure, examen, harmonisation, analyse, réponse, information.
Utilisation des résultats	Soutien à la planification stratégique, intégration au SMSI	Hiérarchisation des risques, actions correctives ciblées, aide à la décision opérationnelle
Avantages	Alignée aux normes ISO 27001/27002, adaptable à tout secteur.	Méthode outillée, scénarios de risques, pertinence dans des contextes concrets.
Limites	Moins orientée terrain sans outils complémentaires.	Nécessite une bonne maîtrise technique, moins adaptée à un cadre stratégique global.
Intégration possible	Peut être renforcée par MEHARI pour une vision plus opérationnelle.	Complète ISO/IEC 27005 pour une mise en œuvre plus pragmatique.

Source : Élaboration personnelle à partir des entretiens réalisés chez NAFTAL et de l'analyse documentaire.

- **Avantages pour NAFTAL et ses parties prenantes**

L'intégration de la méthodologie MEHARI dans les processus de gestion des risques liés à la cybersécurité permettra à NAFTAL de bénéficier d'une évaluation plus complète et structurée des risques pesant sur la sécurité de l'information. Cette approche contribuera à renforcer la qualité des analyses, tout en assurant une meilleure priorisation des actions de traitement des risques, conformément aux exigences de la norme ISO/CEI 27005.

En combinant les principes directeurs d'ISO/CEI 27005, qui fournit un cadre rigoureux pour la gestion des risques liés à la sécurité de l'information, avec la méthodologie opérationnelle et pragmatique de MEHARI, NAFTAL peut mettre en place un dispositif de gouvernance IT plus efficace et résilient. Ce couplage permet non seulement d'aligner la gestion des risques sur les objectifs stratégiques de l'entreprise, mais aussi de répondre aux attentes des parties prenantes en matière de conformité, de performance et de sécurité.

L'adoption d'une telle démarche renforce également l'image de NAFTAL en tant qu'organisation proactive et alignée sur les meilleures pratiques internationales, tout en facilitant les audits internes et externes grâce à une traçabilité claire et documentée des analyses de risques et des mesures de sécurité mises en œuvre.

2.Résultats

2.1 Résultats d'observation

L'observation directe de la Direction des Systèmes d'Information (DSI) de NAFTAL a permis d'évaluer concrètement les pratiques en matière de cybersécurité, les menaces actuelles prises en compte, les vulnérabilités existantes, les outils techniques disponibles, ainsi que les comportements organisationnels. Une immersion sur le terrain, dans les conditions réelles de travail, a facilité une appréciation objective de l'efficacité des dispositifs de sécurité existants et de leur conformité aux principes de gouvernance IT.

L'attention a été portée sur plusieurs actifs critiques, notamment le site web de e-paiement, la base de données des ressources humaines, les postes de travail des utilisateurs, les comptes mails professionnels, ainsi que les accès administrateurs au site WordPress. Ces éléments ont été analysés dans leur contexte d'utilisation afin de déterminer leur niveau de sensibilité, leur exposition, ainsi que leur mode d'exploitation par les équipes concernées.

- **Constatations principales**

Une sensibilité élevée a été constatée pour certains actifs, en particulier la base de données RH (données personnelles) et le site de e-paiement (point d'entrée client et activité financière).

Les observations ont permis d'identifier plusieurs vulnérabilités critiques au sein du système d'information de NAFTAL. Parmi celles-ci figurent la faiblesse des mots de passe utilisés pour les comptes administrateurs, l'absence d'authentification multi facteur (MFA) sur les

systèmes sensibles, ainsi que des mises à jour irrégulières de la plateforme WordPress. À cela s'ajoute l'absence de sauvegardes automatiques dans la zone DMZ, ce qui augmente considérablement le risque de perte de données en cas d'attaque. Par ailleurs, il a été constaté un manque de formation en cybersécurité auprès des employés, ce qui les rend plus vulnérables face aux menaces.

En ce qui concerne les menaces identifiées, l'environnement est exposé à plusieurs types d'attaques : des campagnes de phishing ciblent les employés à travers des e-mails frauduleux, tandis que les ransomwares représentent une menace réelle en tentant de chiffrer les postes utilisateurs. Des vulnérabilités dans les formulaires web laissent place à des attaques par injection SQL, et les accès administrateurs restent exposés en raison de mots de passe faibles ou compromis. Enfin, le site web peut être perturbé par des attaques par déni de service distribué (DDoS), compromettant ainsi sa disponibilité.

Tableau 5: Tableau des risques**.**

Risque	Impact	Probabilité	Niveau de risque
Fuite de données clients	Critique	Moyenne	Élevé
Compromission admin web	Élevé	Élevée	Critique
Ransomware sur postes	Élevé	Moyenne	Élevé
Phishing réussi	Modéré	Élevée	Élevé
DDoS sur le site	Modéré	Faible	Modéré

Source : Document interne de NAFTAL.

- **Actions recommandées et initiatives existantes**

- Mettre en œuvre l'authentification multi facteur (MFA), imposer la rotation des mots de passe et journaliser les connexions ;
- Automatiser les sauvegardes et chiffrer les informations sensibles ;
- Mettre en place une politique de sensibilisation et de formation des utilisateurs à la cybersécurité ;
- Installer une protection anti-DDoS dédiée ;

- Surveiller les indicateurs de performance tels que le pourcentage d'employés formés ou le nombre de comptes protégés par MFA.

Un plan d'action a été lancé, avec une répartition des responsabilités (DSI externe, responsable e-commerce, RH), un délai de mise en œuvre compris entre 1 et 3 mois, et une révision des risques tous les 6 mois.

Cette observation révèle un cadre de gouvernance encore en cours de structuration, au sein duquel plusieurs projets sont en cours afin de combler l'écart entre les capacités actuelles de l'organisation et les besoins en matière de cybersécurité. Elle confirme la nécessité d'une approche globale, combinant solutions techniques, mécanismes de gouvernance et sensibilisation des utilisateurs, pour lutter efficacement contre les menaces cyber.

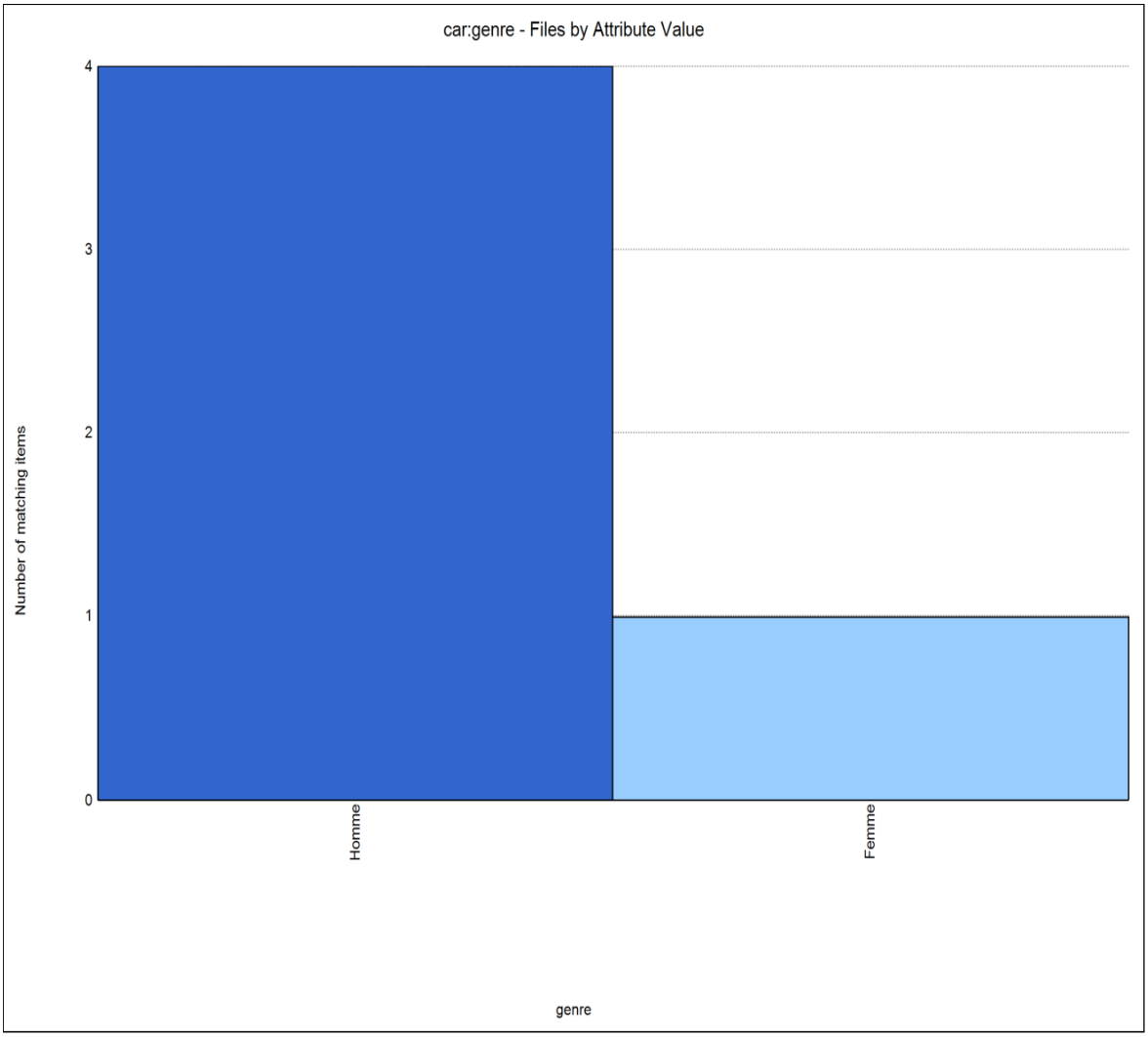
2.2. Résultats d'entretiens

Dans le cadre de cette recherche, nous avons réalisé cinq entretiens semi-directifs avec des professionnels exerçant au sein de NAFTAL, afin d'évaluer comment un cadre structuré de gestion des risques de cybersécurité peut être intégré dans une approche globale de gouvernance IT. L'objectif était de recueillir des témoignages concrets sur les pratiques actuelles, les méthodes d'évaluation des risques, ainsi que sur la pertinence d'outils comme la méthode MEHARI dans ce contexte.

Nous avons analysé les réponses recueillies, comparé les points de vue exprimés et organisé les résultats autour de plusieurs axes, permettant de relier les pratiques de cybersécurité aux enjeux stratégiques et organisationnels de NAFTAL.

Pour mieux comprendre notre échantillon, nous avons créé plusieurs représentations visuelles à l'aide de l'outil d'analyse NVivo10.

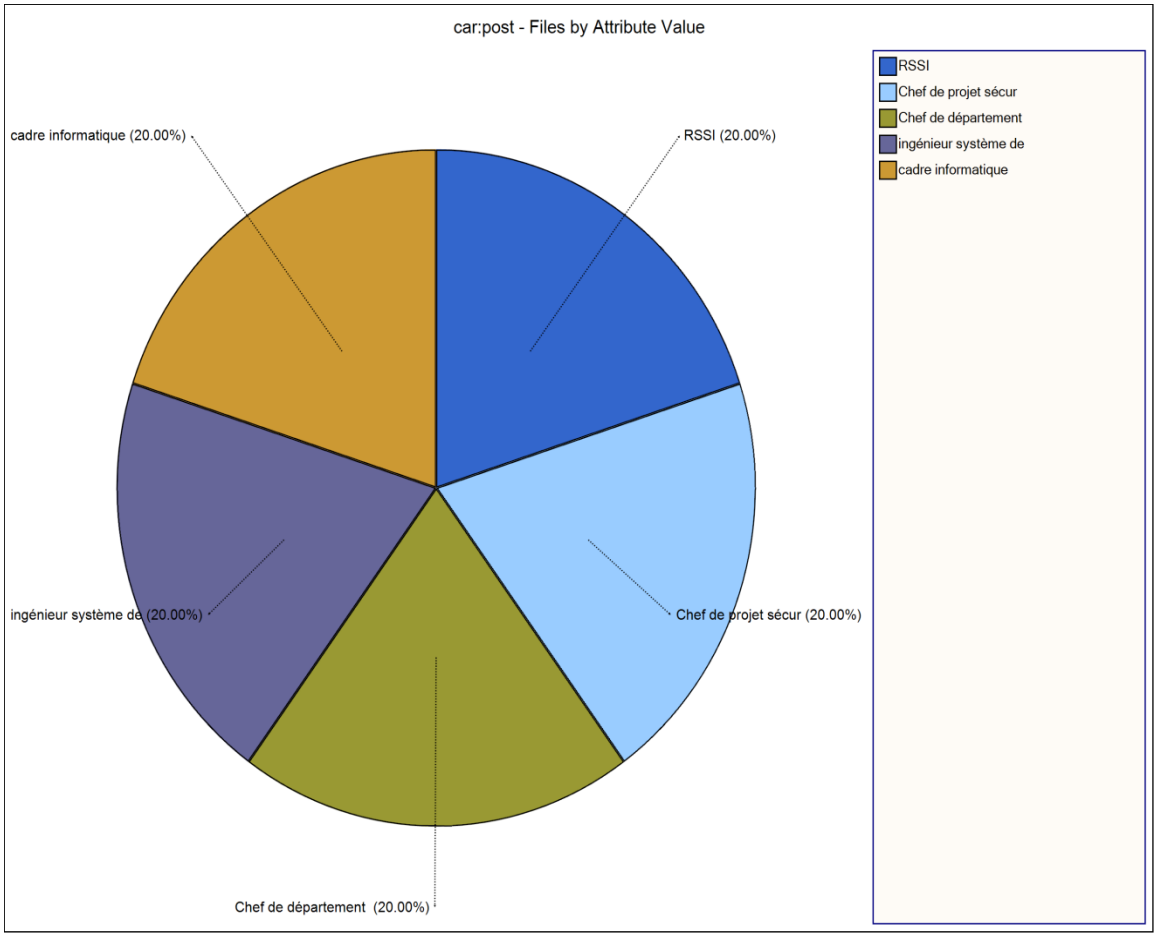
Figure 11 : Genre des employés.



Source : (NVivo, 2010).

Le diagramme montre une prédominance des hommes (80 %) par rapport aux femmes (20%) dans l'échantillon. Ce déséquilibre pourrait influencer les résultats de l'analyse.

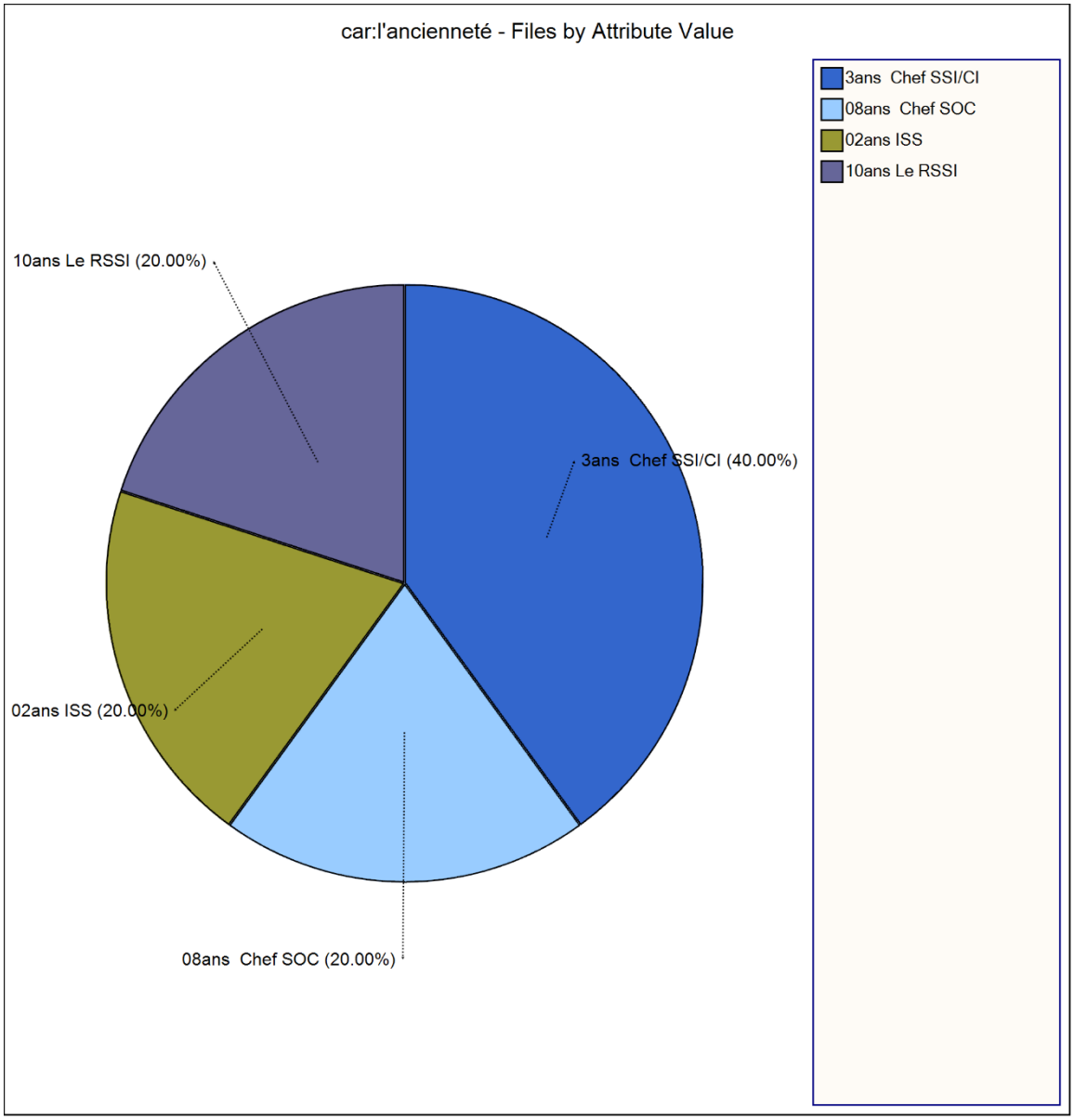
Figure 12 : post des employés.



Source : (NVivo, 2010).

Le tableau montre une répartition équitable entre les postes, chacun représentant 20 % de l'échantillon : RSSI (Responsale de sécurité de système d'information, ingénieur système de sécurité, Chef de projet sécurité, Chef de département SOC et cadre informatique Niv3.

Figure 13 : l'ancienneté des employés.



Source : (NVivo, 2010).

Le graphique en barres illustre la répartition de l'ancienneté parmi les répondants, avec une prédominance de 3 ans d'expérience, comme c'est le cas pour un chef de projet sécurité SI et un cadre informatique niveau 3, tous deux ayant 3 ans dans leurs fonctions. On note également un chef de département SOC totalisant 8 ans d'ancienneté, dont 5 ans spécifiquement dans le domaine de la sécurité SI, ainsi qu'un ingénieur système de sécurité avec 2 ans d'expérience. Cette distribution reflète une majorité de profils ayant une expérience récente à moyenne dans l'organisation.

2.2.1. L'analyse globale des entretiens

Avant de procéder à l'analyse approfondie des données issues des entretiens, il est essentiel d'évaluer la cohérence globale entre les réponses des participants et les thématiques centrales de cette recherche. À l'aide de l'outil d'analyse de corrélation de NVivo, un tableau été générée afin d'examiner la similarité entre les entretiens sur la base de la structure de codage. Les résultats révèlent une corrélation généralement forte entre le fichier de référence (« les Réponses 1 ») et plusieurs entretiens, notamment l'entretien 2 (r = 0,81), l'entretien 4 (r = 0,71) et l'entretien 5 (r = 0,64). Cela indique un chevauchement thématique significatif, suggérant que les participants abordent des enjeux directement liés à l'objectif de recherche. De plus, les fortes inter-corrélations entre les entretiens (par exemple, entretien 5 & entretien 4 : r = 0,77) reflètent une cohérence des récits, renforçant la pertinence des codes retenus. Enfin, les corrélations modérées avec certains entretiens mettent en lumière des points de vue variés, qui contribuent à une compréhension plus nuancée du sujet traité.

Figure 14: Items clustered by word similarity.

Source : (NVivo, 2010).

Tableau 6: Items clustered by word similarity.

File A	File B	Pearson correlation coefficient
Files\\les Réponses 1	Files\\interview 2	0.814836
Files\\interview 5	Files\\interview 4	0.769057
Files\\interview 4	Files\\interview 3	0.737068
Files\\interview 5	Files\\interview 3	0.726691
Files\\interview 4	Files\\interview 2	0.723831
Files\\les Réponses 1	Files\\interview 4	0.70647
Files\\les Réponses 1	Files\\interview 5	0.639885
Files\\interview 5	Files\\interview 2	0.633663
Files\\interview 3	Files\\interview 2	0.562351
Files\\les Réponses 1	Files\\interview 3	0.543532

Source: (NVivo, 2010).

Dans la continuité de l'analyse des corrélations, une analyse de fréquence des mots a été menée afin de repérer les termes les plus récurrents dans les entretiens. Cette étape permet d'identifier rapidement les notions les plus évoquées par les participants et d'appuyer les thématiques ressorties lors du codage.

Figure 15 : Nuage de mots.

Source: (NVivo, 2010).

Tableau 7: Word Frequency Query Results.

Word	Length	Count	Weighted Percentage (%)	Similar Words
l'alignement	12	34	1.21	L'accès, l'adapter, l'ajustement, l'alignement, l'analyse, l'efficacité, l'ensemble, l'entreprise, l'équipe, l'état, l'évaluation, l'exploiter, l'intérêt
Direction	9	30	1.02	Charge, direction, directions, directives, management, organisation, points
D'évaluation	12	28	1.00	D'abord, d'alerte, d'amélioration, d'après, d'évaluation, d'évolution, d'expérience, d'exposition, d'impact, d'incidents, d'inclure, d'intégrer, d'investissements
risques	7	24	0.85	risque, risques
surtout	7	20	0.71	surtout
sécurité	8	20	0.71	sécurité
gouvernance	11	18	0.64	gouvernance
critiques	9	14	0.50	critiques
gestion	7	14	0.50	gestion
métiers	7	14	0.50	métier, métiers
systèmes	8	14	0.50	systèmes
interne	7	12	0.43	externe, interne, internes
manque	6	12	0.43	manque
parfois	7	12	0.43	parfois
stratégie	9	12	0.43	stratégie
vulnérabilités	14	12	0.43	vulnérabilités
formations	10	12	0.38	formation, formations, organisation
approche	8	10	0.36	approche
certains	8	10	0.36	certaines, certains
incidents	9	10	0.36	incident, incidents

Source : (NVivo, 2025).

L'analyse des mots les plus utilisés dans les entretiens montre ce qui est le plus important pour les participants concernant la gouvernance IT et la cybersécurité chez NAFTAL. Le mot « l'alignement » revient 34 fois, ce qui indique que beaucoup insistent sur la nécessité d'aligner la stratégie IT avec les objectifs globaux de l'entreprise. Juste après, « direction » est mentionné 30 fois, ce qui reflète l'importance du rôle de la direction dans la mise en place de cette gouvernance, le mot « d'évaluation » apparaît 28 fois, montrant que les participants

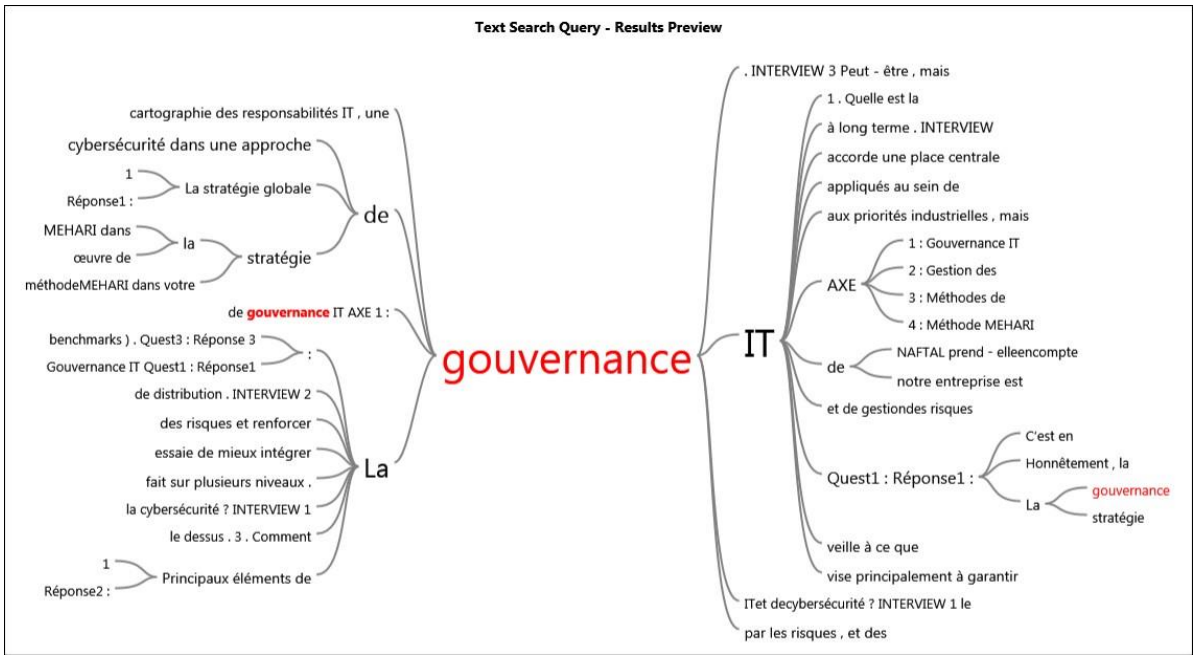
accordent une grande importance à l'évaluation des risques et des dispositifs existants. Les termes « risques » (24 fois) et « sécurité » (20 fois) sont également très présents, ce qui confirme que la gestion des risques et la cybersécurité sont des sujets majeurs dans les préoccupations des répondants, d'autres mots comme « gouvernance », « gestion », « systèmes », ou encore « métiers » sont souvent cités, ce qui montre un intérêt pour l'organisation, les pratiques internes, et les responsabilités métiers liées à la cybersécurité. Enfin, des mots comme « vulnérabilités », « incidents », ou « formations » soulignent les faiblesses à corriger et le besoin de renforcer les compétences internes pour mieux faire face aux cybermenaces.

Globalement, cette analyse montre que les participants perçoivent la gouvernance IT comme un levier stratégique, mais qu'elle doit être soutenue par une direction impliquée, une bonne évaluation des risques, et des actions concrètes sur le terrain.

2.2.1.1. Gouvernance IT

- **Stratégie et alignement avec les objectifs de l'entreprise**

Figure 16: Text Search Query - Results Preview gouvernance.



Source : (NVivo, 2025).

Les réponses recueillies offrent une vision partagée mais nuancée de la stratégie globale de gouvernance IT à NAFTAL. D'un côté, certains participants décrivent une organisation structurée et orientée vers des objectifs clairs. Par exemple, l'un d'eux souligne que la stratégie est *« centralisée, encadrée par des directives gouvernementales et orientée vers l'intérêt général »* (Entretien 1), avec une volonté d'améliorer la productivité, de réduire les pertes et d'optimiser les processus industriels. Cette approche met en avant un alignement entre les systèmes IT et les grandes priorités de l'entreprise. D'autres réponses confirment cette orientation, en insistant sur des objectifs plus techniques ou sectoriels. L'IT est perçue comme un levier de *« résilience des systèmes critiques »* et de *« sécurité énergétique »* (Entretien 2), ce qui témoigne d'une intégration progressive dans la stratégie de performance et de modernisation de NAFTAL. Ces éléments indiquent que certains aspects de la gouvernance IT sont bien alignés avec les objectifs globaux de l'entreprise. Malgré ces points positifs, plusieurs répondants soulignent des écarts entre la stratégie théorique et sa mise en pratique. Par exemple, l'un indique que *« l'alignement avec les priorités industrielles est en cours, mais pas encore totalement structuré »* (Entretien 3), tandis qu'un autre reconnaît que *« la stratégie est surtout présente sur le papier »* (Entretien 5). Ces remarques mettent en évidence des défis dans l'application concrète de la gouvernance IT. Il est également mentionné que des efforts sont en cours pour combler ces lacunes. Comme le souligne un participant, *« l'alignement se fait progressivement, ce n'est pas encore parfait »* (Entretien 4), ce qui montre une volonté d'adaptation continue, même si des ajustements restent nécessaires pour une intégration plus cohérente des objectifs IT dans la stratégie globale de l'entreprise.

- **Pratiques et éléments de gouvernance IT au sein de la DSI**

Les réponses des participants montrent plusieurs pratiques importantes en matière de gouvernance IT au sein de la DSI de NAFTAL. Tout d'abord, plusieurs insistent sur l'importance de faire en sorte que les projets informatiques soient bien liés aux objectifs de l'entreprise. Comme le dit un participant (Entretien 1), il s'agit de *« mettre en cohérence les projets IT avec les objectifs métiers et stratégiques de l'entreprise »*, comme la production, la sécurité ou la transition énergétique. Cela montre que l'IT n'est pas utilisée seule, mais sert à soutenir les grandes priorités de NAFTAL. Ensuite, la collaboration avec les autres services est souvent citée. Le même répondant parle d'un *« travail collaboratif avec les directions métiers »* pour bien comprendre les besoins et y répondre. D'autres (Entretien 3)

évoquent aussi le rôle des *comités de pilotage* pour suivre les projets les plus importants, même si ce n'est pas toujours fait de façon régulière. Cela montre que, même si la collaboration existe, elle peut parfois manquer de régularité. L'amélioration continue est un autre point souvent mentionné. Des pratiques comme les audits, les retours d'expérience ou les comparaisons avec d'autres entreprises (benchmarks) sont utilisées pour améliorer les projets IT (Entretien 1). Le suivi à travers des tableaux de bord et des indicateurs est aussi évoqué (Entretien 4), ce qui permet de mieux contrôler l'avancement des projets. Cependant, certains répondants notent des limites. Par exemple, un participant (Entretien 5) dit que *« parfois ça reste très théorique »* et que les situations urgentes prennent souvent le dessus. Cela montre que, même si un cadre existe, il n'est pas toujours facile à appliquer dans la réalité. Enfin, un autre point important est la *gouvernance par les risques*, mentionnée dans l'Entretien 2. Il s'agit ici d'intégrer les risques dans la gestion des projets IT, avec des indicateurs de performance revus en réunion de direction. Cela montre une approche plus structurée, même si, dans la pratique, tout n'est pas encore parfaitement en place.

En résumé, les participants parlent d'un cadre de gouvernance IT globalement bien pensé, mais qui peut être difficile à appliquer de manière régulière à cause de contraintes de terrain et du manque de temps ou de moyens.

- **Intégration des risques de cybersécurité dans la gouvernance IT**

Les réponses montrent que NAFTAL prend en compte les risques liés à la cybersécurité dans sa gouvernance IT, mais pas toujours de la même manière. Pour certains, la cybersécurité est une priorité claire. Par exemple, un participant (Entretien 1) explique que *« la gouvernance IT accorde une place centrale à la gestion des risques cyber »*, car la sécurité est importante pour faire fonctionner les installations industrielles et protéger les intérêts du pays. D'autres (Entretien 2) indiquent qu'il existe un comité spécial qui suit les risques numériques, ce qui montre qu'il y a des efforts pour intégrer la cybersécurité dans la stratégie globale de l'IT. Cependant, plusieurs remarques montrent aussi que cette prise en compte est parfois incomplète. Par exemple, un participant (Entretien 3) dit que les risques cyber sont bien pris en compte, *« surtout depuis les derniers incidents régionaux »*, mais qu'il manque souvent de coordination entre les équipes IT et les autres services. Un autre (Entretien 4) reconnaît que la cybersécurité est présente, mais souvent en réponse à des alertes ou incidents, donc après coup, et pas forcément de manière préventive.

Enfin, un participant (Entretien 5) ajoute que la direction générale soutient surtout quand il y a des urgences ou des demandes critiques, mais qu'elle reste distante le reste du temps.

- **Implication de la direction générale dans la gouvernance IT**

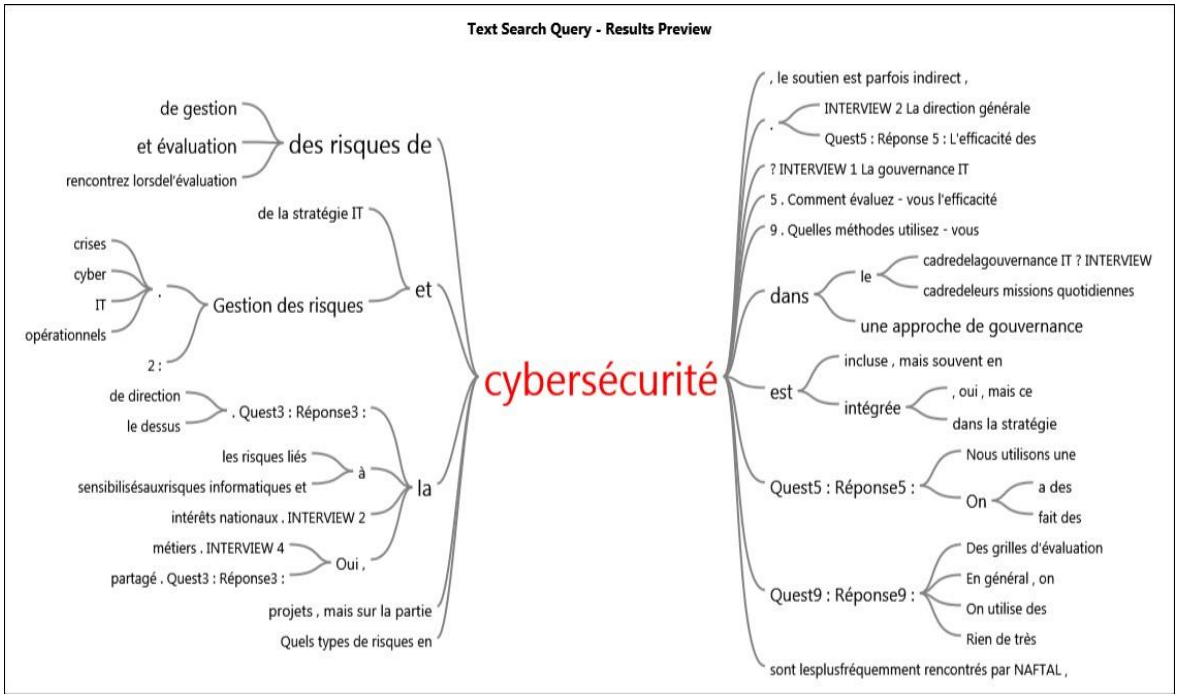
Les réponses à cette question montrent que la direction générale (DG) de NAFTAL joue un rôle important, mais parfois limité, dans la mise en œuvre de la stratégie de gouvernance IT et de cybersécurité. Pour certains participants, ce rôle est clairement stratégique. Par exemple, un répondant affirme que *« le soutien de la direction générale est essentiel pour assurer la crédibilité, l'efficacité et la pérennité »* de la stratégie IT (Entretien 1), ce qui montre que sans un appui fort de la DG, il serait difficile de faire avancer les projets importants. D'autres précisent que la direction générale agit comme un *sponsor* (Entretien 2): elle approuve les budgets et donne la priorité aux projets qui présentent de grands enjeux en matière de cybersécurité. Cela signifie qu'elle joue un rôle dans les décisions clés, notamment au moment de choisir quels projets financer ou soutenir. Cependant, plusieurs répondants soulignent que ce soutien n'est pas toujours constant ou direct. Par exemple, l'un explique que *« sur la partie cybersécurité, le soutien est parfois indirect, surtout en dehors des crises »* (Entretien 3), ce qui laisse entendre que la DG s'implique davantage en cas de problème. De la même manière, d'autres précisent que la direction est surtout présente lorsqu'il s'agit de grands investissements (Entretien 4), ou bien quand il y a des incidents ou des situations urgentes (Entretien 5), mais qu'elle reste plutôt éloignée des activités informatiques du quotidien.

Au final, on peut dire que la DG a un rôle de décisionnaire et de soutien, surtout pour les aspects stratégiques et financiers. Mais dans la gestion courante de la cybersécurité et des projets IT, son implication reste partielle ou ponctuelle, ce qui peut parfois limiter la portée des efforts de gouvernance IT sur le terrain.

2.2.1.2. Gestion des risques et cybersécurité

➢ **Évaluation des processus de gestion des risques informatiques**

Figure 17: Text Search Query - Results Preview cybersécurité.



Source : (NVivo 2025).

Les réponses à cette question montrent que l'évaluation de l'efficacité des processus de gestion des risques informatiques dans l'entreprise varie en fonction des approches et des pratiques utilisées au sein de la DSI. Un participant (Entretien 1) note que, bien que des processus existent, leur efficacité dépend en grande partie de la *« charge de travail et des priorités du moment »*. Cela suggère que l'évaluation peut être influencée par des facteurs externes ou urgents, ce qui pourrait limiter une évaluation continue et approfondie des risques. Un autre répondant (Entretien 2) mentionne l'utilisation d'une *« matrice de criticité »* pour évaluer l'efficacité des dispositifs en place. Cela permet de classer les risques en fonction de leur gravité et de déclencher des actions correctives si nécessaire. Cette approche semble plus structurée et axée sur la réactivité face aux risques identifiés. En revanche, un autre participant (Entretien 3) souligne que l'évaluation reste *« assez classique »*, se basant principalement sur des audits internes. Bien que cette méthode soit courante, elle peut manquer de flexibilité et ne pas toujours refléter l'évolution rapide des menaces informatiques. L'un des répondants (Entretien 4) soulève également un point intéressant

concernant la *« sensibilisation ponctuelle »* des employés aux risques informatiques. Bien qu'il y ait des actions de sensibilisation, il semble qu'il manque un programme structuré et continu pour garantir une prise de conscience constante au sein de l'entreprise. Cette absence de structure pourrait réduire l'efficacité globale des processus, car une sensibilisation régulière est essentielle pour maintenir une vigilance élevée. Enfin, un autre participant (Entretien 5) mentionne une approche plus systématique pour évaluer l'efficacité des processus, combinant des *« référentiels normatifs, audits, exercices de simulation et tests des plans de réponse »* avec une implication active du top management. Cette approche semble plus complète et permet de vérifier régulièrement si les processus sont adaptés et efficaces face aux risques émergents. Cela montre un effort pour avoir une évaluation rigoureuse et intégrée des risques.

Dans l'ensemble, bien que des méthodes variées existent, il apparaît que l'évaluation des processus de gestion des risques informatiques chez NAFTAL reste inégale et dépend de la situation et des priorités du moment. Une approche plus systématique et continue pourrait renforcer l'efficacité globale des dispositifs en place.

- **Typologie des risques rencontrés et modes de gestion**

Les risques de cybersécurité rencontrés par NAFTAL sont variés et souvent liés à des vulnérabilités courantes dans le domaine de l'informatique. Parmi les risques les plus fréquemment mentionnés par les répondants, le phishing et les attaques liées à des logiciels non mis à jour reviennent régulièrement. Par exemple, un répondant (Entretien 1) parle de *« phishing, logiciels non mis à jour, et accès non maîtrisés sur certains équipements »*, tandis qu'un autre mentionne spécifiquement les attaques par *« phishing ciblé et compromission des comptes utilisateurs »* (Entretien 2). Ces types d'attaques sont des risques classiques pour de nombreuses entreprises et témoignent de la nécessité de maintenir des mesures de sécurité à jour. Les réponses montrent que la gestion de ces risques se fait souvent de manière réactive, avec des actions comme des campagnes de sensibilisation pour lutter contre le phishing (Entretien 2), ou des actions de sécurité plus techniques comme la gestion des vulnérabilités logicielles et le lancement de scans réguliers (Entretien 5). Un répondant indique que la gestion des risques reste parfois *« manuelle sur certains points »* (Entretien 1), ce qui suggère que des processus automatisés ou plus structurés ne sont pas toujours mis en place, laissant place à des interventions manuelles qui peuvent être moins efficaces.

Concernant les mesures de gestion mises en place, plusieurs répondants mentionnent des outils classiques tels que les antivirus, les VPN, ou encore les sauvegardes régulières. Un participant (Entretien 4) précise qu'ils ont récemment renforcé l'accès physique aux serveurs pour limiter les risques. De plus, un autre répondant (Entretien 5) parle de stratégies plus spécifiques comme la *« segmentation réseau »* pour limiter la propagation d'attaques, ou l'élaboration d'un *« plan de réponse à incident »* avec un scénario de ransomware, ce qui montre une prise de conscience des risques graves et une volonté de se préparer à des situations critiques. Un autre aspect important de la gestion des risques est le renforcement de l'authentification et des mots de passe. Par exemple, plusieurs répondants évoquent des *« mots de passe renforcés »* et l'introduction de la *« double authentification »*, bien que celle-ci ne soit pas encore généralisée dans tous les cas (Entretien 1). De plus, des mesures techniques comme les *« firewalls nouvelle génération »* et le *« durcissement des configurations »* sont également mentionnées (Entretien 2), ce qui montre une volonté de renforcer les défenses contre les attaques extérieures. Malgré ces efforts, certains risques restent plus difficiles à gérer, comme les *« connexions distantes mal sécurisée s»* ou les *« failles dans les applications anciennes »* (Entretien 4), qui continuent de poser des défis à la sécurité des systèmes d'information. Cela montre que, bien que des mesures soient mises en place, des vulnérabilités subsistent, surtout lorsque des systèmes anciens ou mal configurés sont en jeu.

En résumé, les réponses montrent que NAFTAL rencontre des risques de cybersécurité variés, allant des attaques par phishing aux vulnérabilités liées à des logiciels non mis à jour. Les mesures de gestion sont principalement réactives, avec un certain nombre de pratiques classiques mises en place pour limiter les risques, mais des défis demeurent, notamment en termes de gestion des anciennes applications et des vulnérabilités liées aux connexions distantes.

- **Sensibilisation des équipes aux enjeux de cybersécurité**

La sensibilisation des employés de la DSI aux risques informatiques et à la cybersécurité se fait de diverses manières, mais avec des approches qui varient selon les pratiques. Par exemple, un participant mentionne que les employés reçoivent *« quelques rappels, des mails internes »*, bien qu'il n'y ait pas de formations formelles ou continues. Cela montre qu'il existe un effort pour maintenir un certain niveau de sensibilisation, mais que ces actions restent ponctuelles. Un autre répondant fait état de *« ateliers trimestriels de sensibilisation*

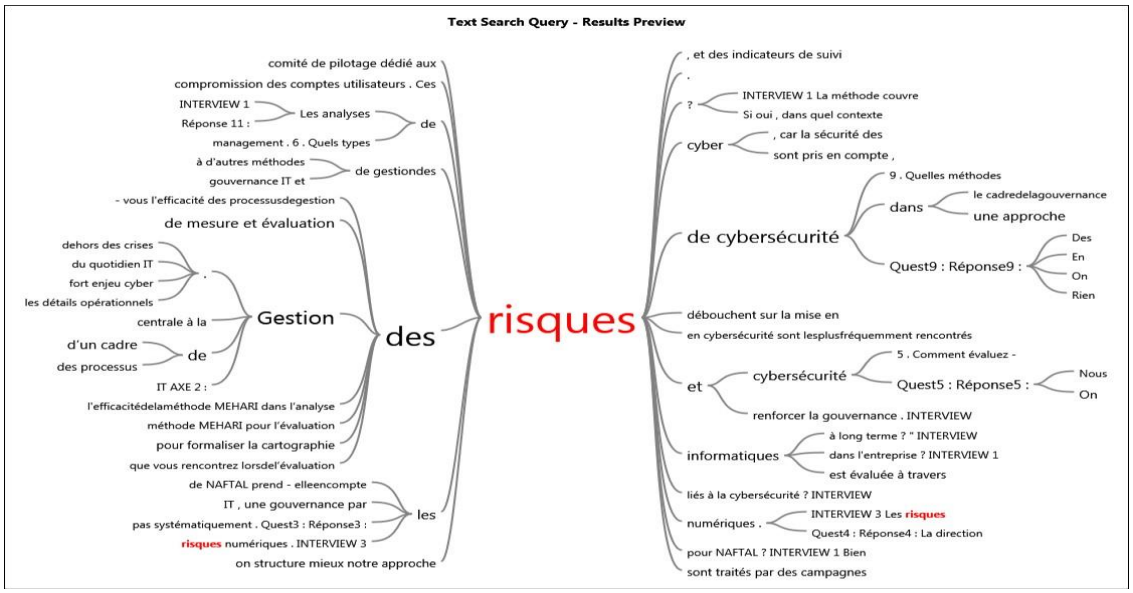
», qui sont axés sur des *« cas concrets d'incidents »*. Cette méthode, plus interactive et pratique, permet aux employés de se confronter à des situations réelles de cybersécurité, ce qui peut être plus concret et marquant. Cependant, ces ateliers étant organisés seulement tous les trois mois, la sensibilisation pourrait être insuffisante pour maintenir un niveau constant de vigilance. Pour un autre participant, la sensibilisation se fait par des *« rappels réguliers »*, mais les formations restent limitées aux profils techniques. Cela suggère que la cybersécurité est abordée de manière plus approfondie avec les membres ayant des compétences techniques, mais que d'autres employés pourraient être moins concernés par ces initiatives.

Dans l'ensemble, il apparaît que les efforts de sensibilisation existent, mais ils varient en termes de fréquence, de format et d'accessibilité, et qu'une approche plus continue et plus inclusive pourrait être bénéfique pour renforcer la cybersécurité au sein de la DSI.

2.2.1.3 Méthodes de mesure et évaluation des risques de cybersécurité

- **Méthodes d'évaluation des risques cyber**

Figure 18: Text Search Query - Results Preview risques.



Source : (NVivo, 2025).

Les méthodes utilisées pour évaluer les risques en cybersécurité au sein de NAFTAL varient d'un répondant à l'autre, ce qui montre une approche diversifiée mais parfois manquant de standardisation. Plusieurs participants évoquent l'utilisation de scans de vulnérabilités et d'audits réguliers, aussi bien internes qu'externes, réalisés avec des partenaires spécialisés (Entretien 1). Ces audits permettent de repérer les failles potentielles et d'évaluer la sécurité des systèmes. En complément, l'utilisation d'outils de gestion des vulnérabilités comme *Vulnerability Management* et des méthodologies telles que *OWASP Top 10* (Entretien 1) permettent de se concentrer sur les risques les plus courants en cybersécurité, en particulier les vulnérabilités critiques. D'autres répondants soulignent l'utilisation de grilles d'évaluation basées sur des normes comme ISO 27005 (Entretien 2), ce qui montre une volonté d'aligner les pratiques avec des standards internationaux pour une gestion rigoureuse des risques. Ces grilles sont souvent complétées par des outils spécifiques, comme Nessus ou Qualys, qui permettent des analyses techniques approfondies des systèmes (Entretien 2 et 3). Ces outils sont largement utilisés pour détecter les vulnérabilités, mais l'un des répondants mentionne que ces analyses ne sont pas systématiques, ce qui peut limiter leur efficacité dans le temps (Entretien 3).

Certaines approches au sein de NAFTAL sont plus personnalisées, avec une méthode interne qui évalue le niveau d'exposition et la criticité des actifs (Entretien 3). Cette méthode est adaptée à l'environnement spécifique de l'entreprise, mais son efficacité pourrait être réduite si elle n'est pas régulièrement mise à jour ou suivie d'une évaluation plus approfondie. Un autre participant mentionne l'utilisation d'Open VAS, ainsi qu'un outil interne pour la cartographie des vulnérabilités, illustrant ainsi une tendance à mélanger des solutions techniques avec des évaluations internes (Entretien 4). Un des répondants souligne que l'évaluation des risques en cybersécurité chez NAFTAL se fait souvent de manière réactive, principalement lorsqu'un problème est détecté ou signalé (Entretien 5). Cette approche réactive présente un inconvénient majeur, car elle dépend d'événements spécifiques plutôt que d'une surveillance proactive continue. Cela peut rendre difficile la détection précoce des vulnérabilités et limiter la capacité à anticiper les cybermenaces Globalement, bien que NAFTAL utilise plusieurs outils et méthodes pour évaluer les risques en cybersécurité, l'absence d'un cadre global standardisé et la gestion souvent réactive des risques pourraient nuire à la cohérence et à l'efficacité de cette démarche à long terme.

- **Utilisation et valorisation des résultats d'évaluation**

Les résultats des évaluations des risques jouent un rôle important dans la gestion de la cybersécurité chez NAFTAL, mais leur utilisation n'est pas toujours uniforme. Selon le premier entretien (Entretien 1), les évaluations de risques mènent à la mise en place ou à l'ajustement de mesures concrètes telles que des *« politiques de sécurité »*, des *« contrôles techniques »* et des *« processus métier »* pour gérer l'accès aux systèmes sensibles. Ces ajustements permettent de répondre de manière structurée aux risques identifiés et d'assurer une meilleure sécurité des systèmes d'information. Un autre point intéressant est mentionné dans l'Entretien 2, où il est expliqué que les résultats des évaluations orientent directement les décisions d'investissement en cybersécurité et sont utilisés pour alimenter les *« tableaux de bord de risque »*. Cela permet aux équipes de suivre les risques en temps réel et d'ajuster les priorités d'investissement en conséquence. Cela montre bien que l'évaluation des risques n'est pas seulement un outil de diagnostic, mais qu'elle influe également sur les choix stratégiques à long terme. Cependant, il semble y avoir des difficultés concernant l'intégration rapide des résultats dans les actions concrètes. Un répondant (Entretien 3) mentionne que bien qu'ils essaient d'intégrer les résultats dans le *« plan de sécurité »*, le suivi des actions est parfois trop lent. Cela indique qu'il peut y avoir des retards ou des obstacles dans la mise en œuvre rapide des mesures nécessaires, ce qui ralentit la réponse aux risques. De plus, plusieurs répondants soulignent que les résultats sont parfois davantage utilisés pour réagir aux incidents, plutôt que pour les prévenir. Par exemple, un participant (Entretien 5) affirme que les résultats servent principalement à *« réagir »* aux problèmes plutôt qu'à *« prévenir »* les menaces. Ce point suggère qu'il pourrait être nécessaire d'adopter une approche plus proactive pour anticiper les risques et éviter qu'ils ne se transforment en crises.

En résumé, bien que les résultats des évaluations des risques soient utilisés pour améliorer la cybersécurité chez NAFTAL, il semble qu'il y ait encore des ajustements à faire pour mieux intégrer ces résultats dans les processus de décision et de prévention.

- **Contraintes rencontrées lors de l'évaluation des risques**

Les difficultés rencontrées lors de l'évaluation des risques de cybersécurité dans le cadre de la gouvernance IT de NAFTAL sont diverses et reflètent des défis à la fois humains, techniques et organisationnels. Un des obstacles principaux mentionnés par plusieurs répondants est le manque de ressources humaines et de compétences spécialisées. Comme le souligne un participant (Entretien 1), *« les limites en ressources humaines et compétences*

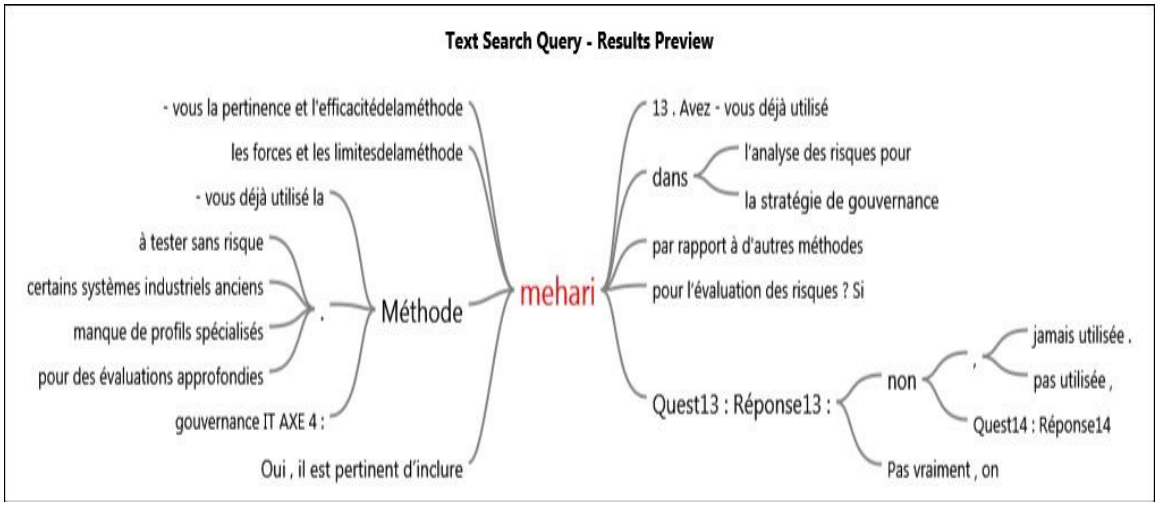
spécialisées » sont un frein important. Cette contrainte est renforcée par le manque de profils spécialisés, comme l'indique un autre répondant (Entretien 3), ce qui rend l'évaluation des risques plus complexe, notamment lorsqu'il s'agit de gérer des systèmes sophistiqués ou de nouvelles menaces. Par ailleurs, un autre défi majeur est lié à l'accès aux données, en particulier dans le contexte de systèmes industriels anciens. Un participant (Entretien 2) explique que *« la difficulté principale est l'accès aux données fiables sur certains systèmes industriels anciens »*. Ces systèmes, souvent peu adaptés aux nouvelles exigences de sécurité, compliquent la collecte et l'analyse des données nécessaires pour évaluer les risques de manière efficace. La coordination entre les différents départements représente aussi un obstacle. Comme le note un répondant (Entretien 3), cette *« coordination entre les départements »* est parfois insuffisante, ce qui peut ralentir ou compliquer l'évaluation des risques. De plus, plusieurs participants mentionnent la contrainte de temps. L'un d'eux (Entretien 4) précise que le manque de temps est un facteur limitant pour effectuer des évaluations approfondies, et un autre (Entretien 5) ajoute que les *« systèmes critiques sont difficiles à tester sans risque »*. Cela suggère qu'une évaluation complète des risques pourrait exposer certains systèmes à des vulnérabilités, rendant l'approche plus délicate.

En somme, les difficultés liées à l'évaluation des risques de cybersécurité sont multiples et interconnectées, avec des ressources humaines limitées, des problèmes d'accès aux données, des défis de coordination, et des contraintes de temps et de sécurité qui compliquent le processus de gestion des risques.

2.2.1.4. Méthode MEHARI

- **Utilisation et connaissance de la méthode MEHARI**

Figure 19: Text Search Query - Results Preview MEHARI.



Source : (NVivo, 2025).

Les réponses à cette question montrent clairement que la méthode MEHARI n'est pas utilisée dans la pratique quotidienne de la DSI de NAFTAL. La majorité des participants répondent simplement *« non »* (Entretiens 1, 2, 5), ce qui indique une absence totale d'application concrète de cette méthode. Même si certains en ont entendu parler, comme le précise un participant: *«Pas vraiment, on en a entendu parler, mais pas utilisée concrètement»* (Entretien 3), ou encore *«déjà mentionnée dans des formations»* (Entretien 4), cela reste au niveau de la connaissance théorique, il est donc évident que MEHARI n'a pas encore trouvé sa place dans les pratiques d'évaluation des risques au sein de l'entreprise, cela peut être dû à un manque de formation approfondie, à la complexité perçue de la méthode, ou simplement à la préférence pour d'autres approches plus connues ou déjà en place, ce constat souligne un écart entre la disponibilité des outils méthodologiques et leur adoption réelle sur le terrain.

- **Appréciation de la pertinence et de l'efficacité de MEHARI**

L'analyse des réponses concernant la pertinence et l'efficacité de la méthode MEHARI dans le contexte de NAFTAL révèle une perception globalement nuancée. Les interviewés reconnaissent plusieurs atouts à cette méthode, tout en soulignant des limites pratiques importantes qui freinent son adoption dans leur environnement spécifique.

La plupart des participants s'accordent à dire que MEHARI est une méthode structurée et complète, ce qui en fait un outil théoriquement solide pour l'analyse des risques. Par exemple, un des répondants affirme qu'elle couvre l'ensemble du cycle de gestion des risques : « identification des biens, des menaces, des vulnérabilités, des mesures existantes, et des impacts », ce qui montre une reconnaissance de sa rigueur méthodologique. Un autre participant ajoute qu'elle est « pertinente pour structurer l'analyse, surtout lorsqu'on manque d'une approche formelle », ce qui souligne son utilité dans des contextes où la gestion des risques n'est pas encore pleinement formalisée.

Cependant, malgré ses qualités théoriques, son application concrète dans une structure comme NAFTAL semble problématique. Plusieurs personnes jugent la méthode trop lourde, complexe ou académique, notamment pour des équipes qui ne sont pas formées spécifiquement à ce type de référentiel. L'un d'eux mentionne que MEHARI « peut paraître rigide ou trop théorique pour des équipes opérationnelles », et un autre insiste sur la nécessité d'un « accompagnement » ou d'un « appui méthodologique fort », notamment dans des environnements « multi-sites ou peu homogènes », comme c'est le cas de NAFTAL.

Un point important ressort également : la méthode est peu connue au sein de l'entreprise. Cela crée un écart entre sa pertinence potentielle et sa faisabilité réelle. Comme le note un répondant, « peut être utile, mais pas connue ici, donc difficile à appliquer ». Ce manque de connaissance et de formation rend son intégration difficile sans un investissement préalable en sensibilisation ou en montée en compétence.

En somme, MEHARI est perçue comme pertinente sur le plan conceptuel, surtout pour structurer une démarche de gestion des risques, mais son poids méthodologique et son manque de flexibilité la rendent difficile à adapter sans ajustements. Pour qu'elle puisse être efficacement intégrée à NAFTAL, il serait nécessaire de prévoir un accompagnement, des formations, et possiblement une simplification adaptée au contexte interne de l'entreprise.

- **Perspective d'intégration de MEHARI à long terme**

Dans le cadre de l'évaluation d'un cadre de gestion des risques de cybersécurité dans une approche de gouvernance IT, les réponses recueillies à la question portant sur l'intégration de la méthode MEHARI dans la stratégie de gouvernance IT à long terme montre une réception globalement favorable, mais teintée de nuances et de conditions, d'un côté, deux des cinq interviewés expriment une adhésion claire à l'idée d'inclure MEHARI dans la stratégie de gouvernance IT. L'un affirme que « oui, il est pertinent d'inclure MEHARI dans la stratégie de gouvernance IT à long terme », ce qui montre une confiance directe dans la méthode. Un autre renforce cette position en ajoutant que MEHARI serait surtout utile pour « formaliser la cartographie des risques et renforcer la gouvernance », cela indique une perception de valeur ajoutée en matière de structuration et de lisibilité des risques, ce qui est essentiel pour une gouvernance IT efficace. À l'inverse, les autres réponses apportent une vision plus prudente ou conditionnelle. Un répondant souligne l'importance de la formation et de l'expérimentation progressive, en disant : « Peut-être, mais il faudrait d'abord former les équipes et tester sur un périmètre limité », cela révèle un souci pragmatique de montée en compétence avant tout déploiement large, un autre mentionne qu'il serait nécessaire de «l'adapter aux réalités du terrain», ce qui montre une conscience des contraintes opérationnelles spécifiques à NAFTAL, qui pourraient ne pas correspondre entièrement à une application rigide de la méthode. Enfin, une réponse plus réservée évoque la possibilité d'adopter MEHARI «sur le long terme, si on structure mieux notre approche risques», soulignant une immaturité actuelle dans la gestion des risques, dans l'ensemble, l'interprétation de ces réponses indique que, bien que la méthode MEHARI soit considérée comme pertinente et potentiellement bénéfique, sa mise en œuvre nécessiterait un accompagnement méthodologique, des adaptations locales, et un certain degré de préparation organisationnelle. Cette prudence démontre une conscience réaliste des défis liés à l'intégration de cadres formels dans des contextes opérationnels complexes, mais aussi une ouverture stratégique vers l'amélioration de la gouvernance IT par une gestion plus rigoureuse des risques cybersécurité.

Section 2 : Discussion des résultats

Cette section vise à mettre en perspective les résultats obtenus à la lumière de la littérature académique, des entretiens réalisés et des observations directes effectuées sur le terrain. Elle permet de confronter les pratiques observées chez NAFTAL aux cadres théoriques et

normatifs en matière de cybersécurité et de gouvernance IT. À travers cette analyse croisée, il s'agit de dégager les principaux écarts, points de convergence et axes d'amélioration. La section se conclut par un ensemble de recommandations concrètes et adaptées au contexte organisationnel de NAFTAL.

2.1. Comparions entre la littérature, les entretiens et l'observation directe

Les données recueillies à NAFTAL par observation directe et entretiens révèlent des dynamiques internes subtiles en matière de cybersécurité, gestion des risques et gouvernance IT. La confrontation de ces résultats avec les modèles issus de la littérature permet d'identifier à la fois des convergences, des divergences, ainsi que des pistes d'amélioration.

2.1.1. Cybersécurité : Écart entre formalisation stratégique et réalité du terrain
Les travaux de Ramdane (2021) mettent en lumière les limites d'une gouvernance cyber peu opérationnelle en Afrique（(Ramdane, 2021). C'est également le cas chez NAFTAL : les entretiens montrent une reconnaissance stratégique de la cybersécurité, mais l'observation confirme des faiblesses concrètes telles que l'absence d'authentification multifacteur (MFA), des mots de passe faibles et des systèmes peu mis à jour. Cela illustre un décalage entre discours et pratiques, souvent présenté dans la littérature comme un frein à la résilience organisationnelle.

2.1.2. Gestion des risques : Outils présents mais usage fragmenté et peu coordonné
La littérature (KERRAOUS, 2020) souligne l'importance des cadres normatifs (ISO 27001, ISO 22301) et d'approches intégrées. Sur le terrain, l'observation a permis d'identifier l'usage d'outils comme Nessus, Open VAS et Qualys. Cependant, les entretiens révèlent que ces outils sont utilisés de façon cloisonnée selon les services, sans politique commune réelle. L'analyse croisée souligne donc un besoin de standardisation et de gestion centralisée, comme le recommande Pöyhönen et *al*. (2022).

2.1.3. Gouvernance IT : Implication stratégique de la direction mais visibilité opérationnelle limitée

Le Référentiel National de Sécurité de l'Information **(**Ministère de la Poste et des Télécommunications., 2020) recommande un engagement clair de la direction via des comités et un RSSI structurant. Les entretiens confirment le soutien stratégique de la haute direction, mais l'observation quotidienne montre que les décisions opérationnelles sont

souvent reportées ou improvisées. Ceci reflète une gouvernance cloisonnée, où l'absence de relais intermédiaires (référents sécurité) limite la mise en œuvre fluide des politiques cyber.

2.1.4. Méthode MEHARI : Méthode connue mais encore peu appliquée

Bien que les répondants reconnaissent l'intérêt méthodologique de MEHARI, la majorité admettent ne pas l'utiliser. L'observation confirme l'absence de grilles MEHARI ou de documentation structurée basée sur cette méthode. Ce manque s'explique par un déficit de formation et une complexité perçue, comme l'indiquent aussi Victor et al. (2024). Une adoption progressive et adaptée via des projets pilotes restreints pourrait constituer une solution viable.

2.1.5. Culture cyber : Initiatives ponctuelles, dépendantes de l'expérience personnelle

L'étude de **(**Putro, 2024) insiste sur le rôle des facteurs humains. Sur le terrain, les entretiens montrent des efforts de sensibilisation occasionnels, tandis que l'observation révèle que les pratiques de sécurité dépendent fortement de l'expérience passée des agents (exposition à une attaque, panne, etc.). Ainsi, une idée originale issue de cette analyse est de développer un réseau interne d'ambassadeurs cyber afin de diffuser les bonnes pratiques entre pairs.

La synthèse conjointe des entretiens, de l'observation et de la littérature spécialisée révèle une cohérence générale sur les enjeux mais aussi des ruptures dans la mise en œuvre. La valeur ajoutée de ce travail réside dans l'approche intégrée adoptée, qui combine sources théoriques, pratiques observées et représentations internes pour proposer des pistes d'amélioration concrètes adaptées au contexte de NAFTAL.

2.2. Recommandations

Tableau 8 : Tableau de synthèse des recommandations.

Axe stratégique	Recommandation	Commentaires / Justification
1. Gouvernance IT	Créer un comité de gouvernance IT/ cybersécurité rattaché à la direction générale.	Permet de renforcer la supervision stratégique conformément aux recommandations du RNSI 2020.
	Intégrer la cybersécurité dans les comités stratégiques et les tableaux de bord de performance.	Favorise une meilleure visibilité des enjeux cyber dans la gestion globale de l'entreprise.

	Nommer un RSSI interne avec un rôle clairement défini en coordination, alerte et reporting.	Assure une continuité et une responsabilité claire dans la gestion quotidienne de la cybersécurité.
2. Évaluation des risques	Déployer un cadre unifié basé sur ISO 27005, NIST ou MEHARI.	Garantit la cohérence des pratiques et facilite les comparaisons inter-départements.
	Standardiser l'usage des outils (Nessus, Qualys, Open VAS) via une politique commune.	Optimise l'utilisation des ressources techniques et améliore la communication entre équipes.
	Planifier des audits réguliers et des simulations de crise.	Permet de tester la résilience réelle du système face aux menaces.
3. Culture de la cybersécurité	Mettre en place un programme de sensibilisation continue, multi-format et adapté aux profils.	Renforce l'ancrage des bonnes pratiques à long terme.
	Intégrer la cybersécurité dans les parcours de formation internes, y compris à l'accueil des nouveaux arrivants.	Crée une base commune de compétences dès l'entrée dans l'organisation.
	Suivre des indicateurs de maturité (participation, incidents déclarés, conformité).	Permet de piloter les efforts de sensibilisation de manière mesurable.
4. Méthodes avancées (MEHARI)	Lancer un projet pilote de mise en œuvre sur un périmètre restreint.	Permet de tester l'outil avant un déploiement à grande échelle.
	Former les acteurs-clés à la méthode MEHARI.	Renforce l'appropriation méthodologique des équipes concernées.
	Adapter et simplifier les modules de MEHARI selon les besoins spécifiques de NAFTAL.	Réduit les freins liés à la complexité perçue de la méthode.
5. Coordination inter-équipes	Créer une plateforme partagée pour le suivi des incidents et des vulnérabilités.	Favorise la transparence et la réactivité dans le traitement des problèmes.
	Clarifier les rôles via une cartographie des acteurs de la sécurité (DSI, métiers, partenaires externes).	Facilite la répartition des responsabilités et la coordination des actions.
	Encourager une approche préventive (veille technologique, analyse des failles).	Permet d'anticiper les risques au lieu de réagir une fois les incidents survenus.

Source : Élaboré par l'auteur à partir des résultats de terrain et de la revue de littérature (2025).

CONCLUSION

Nous clôturons cette recherche en récapitulant les objectifs poursuivis, les résultats obtenus et les recommandations formulées. Nous mettons également en lumière les principales limites de ce travail, ainsi que les perspectives qu'il ouvre pour des études futures.

L'objectif général de cette étude était d'évaluer l'efficacité d'une méthode de gestion des risques afin de renforcer la cybersécurité des systèmes d'information de NAFTAL, dans le cadre d'une approche de gouvernance des technologies de l'information. Plus précisément, cette recherche a examiné comment une approche structurée — en l'occurrence la méthode MEHARI — pouvait être adaptée à l'environnement organisationnel de NAFTAL pour identifier, classifier et atténuer les risques pesant sur ses actifs numériques clés.

Dans cette optique, nous avons mobilisé une méthodologie qualitative, reposant sur les outils d'analyse du cadre MEHARI, appliquée à un échantillon d'actifs informatiques sensibles. Cette approche nous a permis d'obtenir une meilleure compréhension de l'exposition de NAFTAL aux risques cyber et de proposer des recommandations personnalisées, alignées avec sa structure et ses objectifs de gouvernance.

Les résultats confirment la pertinence et l'utilité de la méthode MEHARI dans l'identification et la hiérarchisation des menaces en cybersécurité. Bien que cette méthode soit encore peu exploitée dans la pratique de l'audit IT en Algérie, elle présente l'avantage d'être rigoureuse, méthodique et conforme aux standards internationaux tels que l'ISO 27001 et l'ISO 27005. Nos résultats démontrent ainsi son potentiel à renforcer la posture cybersécuritaire des entreprises opérant dans des secteurs d'infrastructure critique.

Du point de vue managérial, cette recherche offre à NAFTAL des outils concrets, en lui fournissant un cadre structuré pour mieux intégrer la gestion des risques dans ses processus stratégiques et décisionnels. Plus largement, elle propose des enseignements utiles pour d'autres organisations algériennes soucieuses d'améliorer leur gouvernance des systèmes d'information.

Nous recommandons donc à NAFTAL et à d'autres structures similaires d'envisager l'adoption de la méthode MEHARI dans leurs cadres de gestion de la cybersécurité, avec les adaptations nécessaires et un accompagnement par des experts qualifiés.

Comme toute recherche, notre étude présente des limites. La principale est le périmètre restreint de l'analyse, qui s'est limité à quelques actifs et à une seule méthode de gestion des

risques. Par ailleurs, l'absence de littérature empirique sur l'usage de MEHARI en Algérie constitue un obstacle à la généralisation des résultats.

Enfin, parmi les perspectives de recherche futures, nous suggérons d'explorer d'autres stratégies de gestion des risques, de réaliser des analyses comparatives et d'étendre le champ d'étude à d'autres actifs ou à d'autres unités d'activité de NAFTAL. Une telle extension permettrait de consolider les résultats et de formuler des recommandations plus robustes et applicables.

REFERENCES BIBLIOGRAPHIQUES

Références bibliographiques

(ITGI), I. T. (2001). Control Objectives for Information and related Technology (COBIT) 3rd Edition. ITGI.

1., C. d. (2021/2022). Support de cours. Master 1 ISIDS, Département d'informatique, Université Batna 2.

Abdelmadjid, M. (2021). Évaluation de la gouvernance IT dans les administrations publiques algériennes. Mémoire de master, Université d'Alger.

Agence nationale de la sécurité des systèmes d'information (ANSSI). (2021). ANSSI Annual Report 2021. ANSSI.

Alberts, C. &. (2002). Managing information security risks: The OCTAVE approach. Carnegie Mellon University, Software Engineering Institute.

Bawden, D. &. (2019). *La gouvernance de l'information et la gestion stratégique des technologies de l'information. Editions Technologiques.*

Berger, P. L. (1996). *The social construction of reality: A treatise in the sociology of knowledge. Anchor Books.*

Bloch, L. &. (2011). *Sécurité informatique (3e éd.). Eyrolles.*

Bloch, L. &. (2011). *Sécurité informatique (3e éd.). Eyrolles.*

Bloch, L. &. (2011). *Sécurité informatique (3e éd.). Eyrolles.*

Boiral, O. (2007). *Normes ISO et environnement: vers une gestion durable? Presses de l'Université Laval.*

Boudriga, N. (2004). *Sécurité des réseaux informatiques. Eyrolles.*

Boudriga, N. (2004). *Sécurité des réseaux informatiques. Eyrolles.*

Braun, V. &. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa.

Caralli, R. A. (2012). Cybersecurity risk management: Mastering the fundamentals using the OCTAVE approach. Software Engineering Institute, Carnegie Mellon University.

CDW. (2017). Move to a risk based security strategy.

CLUSIF. (2010). MEHARI - Méthode harmonisée d'analyse des risques (version 2010). Club de la sécurité de l'information français (CLUSIF).

Creswell, J. W. (2013). *Qualitative inquiry and research design: Choosing among five approaches (3rd ed.). Sage Publications.*

Denzin, N. K. (1978). *The research act: A theoretical introduction to sociological methods (2nd ed.). McGraw-Hill.*

eSecurity Solutions. (2019). Security risk assessments white paper.

European Union Agency for Cybersecurity (ENISA). (2019). Cybersecurity for SMEs: Challenges and Recommendations. ENISA.

European Union Agency for Cybersecurity (ENISA). (2021). ENISA Threat Landscape Report 2021. ENISA.

Farah, J. &. (2018). Méthodes d'analyse de risque pour la sécurité des systèmes d'information. Revue des Sciences et Technologies de l'Information.

Golea, N. E.-H. (2020/2021). Systèmes d'information : Cours, travaux dirigés et travaux pratiques. Département d'informatique, Faculté des mathématiques et informatique, Université de Batna.

Guba, E. G. (1994). *Competing paradigms in qualitative research. In N. K. Denzin & Y. S. Lincoln (Eds.), Handbook of qualitative research.*

Haes, S. D. (2009). An exploratory study into IT governance implementations and its impact on business/IT alignment. Information Systems Management, 26(2), 123–137. https://doi.org/10.1080/10580530902794710.

ISACA. (2021). COBIT 2019 framework: Governance and management objectives. ISACA.

KERRAOUS. (2020). A literature review of the factors that influence the adoption of an Enterprise Risk Management process. Revue Internationale des Sciences de Gestion.

Khidzir, K. A. (2018). Information security requirement: The relationship between cybersecurity risk, confidentiality, integrity, and availability in digital social media. International Journal of Development and Sustainability.

Kvale, S. &. (2009). *InterViews: Learning the craft of qualitative research interviewing (2nd ed.). Sage Publications.*

Lundgren, M. &. (2019). Privacy, cybersecurity and ethics in business: A philosophical approach. Journal of Information Security and Applications,https://doi.org/10.1016/j.jisa.2019.01.002.

Merriam, S. B. (1998). *Qualitative research and case study applications in education (Rev. ed.). Jossey-Bass Publishers.*

Ministère de la Poste et des Télécommunications. (2020). Référentiel National de Sécurité de l'Information (RNSI 2020). République Algérienne Démocratique et Populaire.

Pillou, J.-F. &.-P. (2013). *Tout sur la sécurité informatique (3e éd.). Dunod.*

Pöyhönen, J. H. (2022). *Cybersecurity capability assessment model for critical infrastructure. In Proceedings of the 21st European Conference on Cyber Warfare and Security (ECCWS).*

Putro. (2024). Information system approaches in cybersecurity. Procedia Computer Science.

Reix, R. (2002). *Systèmes d'information et management des organisations (3e éd.). Vuibert.*

Sawant, P. (2020). Holistic approach to information security risk management. International Journal of Engineering Research & Technology (IJERT), 9(7). ISSN: 2278-0181.

Sebri, A. (2022). Sécurité des systèmes d'informations .

Von Solms, R. &. (2013). From information security to cyber security. Computers & Security.

Weick, K. E. (2007). *Managing the unexpected: Resilient performance in an age of uncertainty (2nd ed.). Jossey-Bass.*

Weill, P. &. (2004). *IT governance: How top performers manage IT decision rights for superior results. Harvard Business Press.*

ANSSI (2010). *Méthodologie d'analyse de risque EBIOS.*

ANSSI, (2009). Principes de la sécurité des systèmes d'information, Agence nationale de la sécurité des systèmes d'information.

CDW, (2017). “MOVE TO A RISK BASED SECURITY STRATEGY”.

Center for Internet Security, CIS Community Defense Model v2.0, 2021.

CLUSIF, (2010). MEHARI -Méthode harmonisée d’analyse des risques- (version 2010), Club de la sécurité de l'information français (CLUSIF).

ENISA, Cybersecurity for SMEs, Challenges and Recommendations, European Union Agency for Cybersecurity.

eSecurity Solutions, (2019). “SECURITY RISK ASSESSMENTS WHITE PAPER”.

Information Technology Governance Institute (ITGI). (2001). Control Objectives for Information and related Technology (COBIT) 3rd Edition, Rolling Meadows, IL: IT Governance Institute.

ISACA. (2012). COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. Information Systems Audit and Control Association.

ITGI, (2001) Board briefing on IT governance, Information Systems Audit and Control Foundation.

Ministère de la Poste et des Télécommunications (2020). Référentiel National de Sécurité de l’Information (RNSI 2020). République Algérienne Démocratique et Populaire.

NIST, “Risk Management Framework for Information Systems and Organizations”, December 2018.

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.

Travaux et cours universitaires

Abderrahim Sebri, Cours Sécurité des Systèmes Informatique Support de cours pour Sécurité des Systèmes d’Informations, Master, France, 2022, ffhal-03906396f.

Cours de Cyber Sécurité 1. (2021-2022). Master 1 ISIDS, Département d'informatique, Université Batna 2.

Dr. Nour El-Houda Golea, (2020-2021). « Systèmes d'information », cours, travaux dirigés et Travaux pratiques département d'informatique, faculté des mathématiques et informatique, Batna.

Normes internationales

International Organization for Standardization. (2018). ISO/IEC 27005:2018 – Information technology – Security techniques – Information security risk management. ISO.

International Organization for Standardization. (2022). ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements. ISO.

ISO (2018). ISO/IEC 27005:2018.

ISO (2022). ISO/IEC 27001:2022.

National Institute of Standards and Technology. (2024). Framework for Improving Critical Infrastructure Cybersecurity – Version 2.0. U.S. Department of Commerce.

Sites internet:

https://doi.org/10.1016/j.procs.2024.03.135

https://doi.org/10.51583/IJLTEMAS.2024.130607

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KoCDEA0

https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0

https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0

https://www.c-risk.com/fr/blog/iso-27005

https://www.enisa.europa.eu

https://www.iso.org/standard/27001

https://www.mpt.gov.dz

https://www.pcisecuritystandards.org/about_us/

ANNEXES

Annexe A : Analyse des risques cybersécurité.

1. Périmètre de l'analyse

- **Actifs concernés** : site web de e-payement, base de données RH, serveurs hébergés dans le DMZ
- **Utilisateurs** : employés (comptabilité, marketing, support client), clients, prestataire informatique

---

2. Actifs identifiés

Actif	Sensibilité	Description
Base de données RH	Élevée	Données personnelles
Site web e-PAYEMENT	Élevée	Point d'accès client + transactions
Accès admin WordPress	Moyenne	Gestion du contenu
Poste de travail support	Moyenne	Traitement des commandes
Compte mail professionnel	Moyenne	Réinitialisation mot de passe

---

3. Menaces identifiées

Menace	Description
Phishing	Emails frauduleux ciblant les employés
Ransomware	Chiffrement des postes utilisateurs
Injection SQL	Attaque sur les formulaires du site
Compromission d'accès admin	MDP faible ou fuite de credentials
Déni de service (DDoS)	Indisponibilité du site

---

4. Vulnérabilités constatées

- Mot de passe admin site web trop simple
- Pas de MFA pour l'accès à la solution e-payement
- Mises à jour WordPress irrégulières
- Aucune sauvegarde automatique de la DMZ
- Pas de formation cybersécurité pour les employés

5-6. Évaluation des risques (extrait)

Risque	Impact	Probabilité	Niveau de risque
Fuite de données clients	Critique	Moyenne	Élevé
Compromission admin web	Élevé	Élevée	Critique

Risque	Impact	Probabilité	Niveau de risque
Ransomware sur postes	Élevé	Moyenne	Élevé
Phishing réussis	Modéré	Élevée	Élevé
DDoS sur le site	Modéré	Faible	Modéré

---

7. Mesures recommandées

Risque	Action proposée	Priorité
Compromission admin web	Forcer MFA + rotation MDP + logs	Haute
Fuite de données clients	Sauvegardes automatiques + chiffrement	Haute
Phishing	Sensibilisation + filtre mail avancé	Moyenne
Ransomware	Antivirus + filtrage USB + sauvegardes	Moyenne
DDoS	Protection d'antiDDOS	Basse

---

8. Suivi du plan

- **Responsables désignés** : DSI (externe), Responsable e-commerce, RH (formation)
- **Délai de mise en œuvre** : 1 à 3 mois
- **Revue des risques** : tous les 6 mois
- **Indicateurs de suivi** : nombre de comptes MFA activés, % employés formés, fréquence des sauvegardes

Annexes 2: Le guide d'entretien.

Variable	Questions
Gouvernance IT	1. Quelle est la stratégie globale de gouvernance IT de NAFTAL ? Comment est-elle alignée avec les objectifs de l'entreprise ?
	2. Quels sont les principaux éléments de la gouvernance IT que vous appliquez au sein de la DSI (Direction des Systèmes d'Information) ?
	3. Comment la gouvernance IT de NAFTAL prend-elle en compte les risques liés à la cybersécurité ?
	4. Quel rôle la direction générale de NAFTAL joue-t-elle dans la mise en œuvre de la stratégie de gouvernance IT et de cybersécurité ?
Gestion des risques et cybersécurité	5. Comment évaluez-vous l'efficacité des processus de gestion des risques informatiques dans l'entreprise ?
	6. Quels types de risques en cybersécurité sont les plus fréquemment rencontrés par NAFTAL, et comment sont-ils gérés ?
	7. Quelles sont les principales mesures mises en place pour protéger les systèmes d'information contre les cybermenaces ?
	8. Comment les employés de la DSI sont-ils sensibilisés aux risques informatiques et à la cybersécurité dans le cadre de leurs missions quotidiennes ?
Méthodes de mesure et évaluation des risques de cybersécurité	9. Quelles méthodes utilisez-vous pour évaluer les risques en cybersécurité au sein de NAFTAL ?
	10. Utilisez-vous des outils spécifiques ou des méthodologies pour évaluer la vulnérabilité de vos systèmes d'information face aux cyberattaques ?
	11. Comment les résultats des évaluations des risques sont-ils utilisés pour améliorer la gestion de la cybersécurité chez NAFTAL ?
	12. Quelles sont les difficultés que vous rencontrez lors de l'évaluation des risques de cybersécurité dans le cadre de la gouvernance IT ?
Méthode MEHARI	13. Avez-vous déjà utilisé la méthode MEHARI pour l'évaluation des risques ? Si oui, dans quel contexte ?
	14. Comment évaluez-vous la pertinence et l'efficacité de la méthode MEHARI dans l'analyse des risques pour NAFTAL ?
	15. Quelles sont, selon vous, les forces et les limites de la méthode MEHARI par rapport à d'autres méthodes de gestion des risques ?
	16. Pensez-vous qu'il serait pertinent d'inclure la méthode MEHARI dans votre stratégie de gouvernance IT et de gestion des risques informatiques à long terme ?"

Annexe 3: La matrice à condensée.

	A : axe1	B : axe2	C : axe3	D : axe4
Interview 2 Chef de projet sécurité SI :03ans	La gouvernance IT vise principalement à garantir la résilience des systèmes critiques. Elle est alignée avec les objectifs de performance, de sécurité énergétique et de modernisation des infrastructures. Nous appliquons une cartographie des responsabilités IT, une gouvernance par les risques, et des indicateurs de suivi de performance intégrés aux revues de direction. La cybersécurité est intégrée dans la stratégie IT via un comité de pilotage dédié aux risques numériques La direction générale joue un rôle de sponsor, elle valide les budgets et soutient la priorisation des projets à fort enjeu cyber.	Nous utilisons une matrice de criticité pour évaluer l'efficacité des dispositifs existants et déclencher des actions correctives. Attaques par phishing ciblé et compromission des comptes utilisateurs. Ces risques sont traités par des campagnes de sensibilisation et une surveillance des connexions anormales Mise en place de firewalls nouvelle génération, durcissement des configurations, et journalisation renforcée des accès. Des ateliers trimestriels de sensibilisation sont organisés avec des cas concrets d'incidents.	Des grilles d'évaluation basées sur des standards comme ISO 27005. Oui, nous utilisons Nessus et Qualys pour les analyses techniques. Ces résultats guident les choix d'investissements en sécurité et alimentent les tableaux de bord de risque. La difficulté principale est l'accès aux données fiables sur certains systèmes industriels anciens.	non Elle est pertinente pour structurer l'analyse, surtout lorsqu'on manque d'une approche formelle. Forces : approche complète et gratuite. Limites : trop académique pour des équipes peu formées. Oui, surtout pour formaliser la cartographie des risques et renforcer la gouvernance.

	C’est en cours d’évolution. On essaie de mieux intégrer la gouvernance IT aux priorités industrielles, mais ce n’est pas encore totalement structuré. On suit surtout les projets critiques via des comités de pilotage. Il y a aussi un cadrage avec les directions métiers, mais pas systématiquement. Les risques cyber sont pris en compte, surtout depuis les derniers incidents régionaux. Mais il manque parfois de coordination entre les équipes IT et métiers.	On a des procédures, mais l’évaluation reste assez classique, surtout basée sur les audits internes. Les pannes dues à des attaques de type ransomware ou des erreurs humaines sont les plus fréquentes. On agit surtout en réactif. Authentification renforcée, segmentation partielle du réseau, mais certaines zones restent exposées.	En général, on utilise une méthode maison basée sur le niveau d’exposition et la criticité des actifs. Oui, Nessus, et quelques outils open source, mais parfois les analyses ne sont pas régulières. On essaie d’intégrer les résultats dans le plan de sécurité, mais le suivi est parfois lent. La coordination entre les départements, et le manque de profils spécialisés.	Pas vraiment, on en a entendu parler, mais pas utilisée concrètement. D’après ce que j’ai lu, c’est structuré, mais complexe à mettre en œuvre sans accompagnement. Elle est complète, mais peut paraître rigide ou trop théorique pour des équipes opérationnelles. Peut-être, mais il faudrait d’abord former les équipes et tester sur un périmètre limité.
Interview 3 Chef de département SOC :08ans dont 05ans dans le domaine sécurité SI	La DG soutient les grands projets, mais sur la partie cybersécurité, le soutien est parfois indirect, surtout en dehors des crises.	Il y a des rappels réguliers, mais les formations restent limitées à certains profils techniques.		

Interview 4 Ingénieur système de sécurité :02ans	La stratégie IT vise surtout la continuité des activités. L'alignement avec les objectifs de l'entreprise se fait progressivement, ce n'est pas encore parfait. On applique surtout des politiques de sécurité, des plans de continuité, et un suivi de projets via un tableau de bord partagé. Oui, la cybersécurité est incluse, mais souvent en réaction à des alertes ou incidents. Pas toujours en amont. La direction générale est impliquée pour les grands investissements, mais pas toujours dans les détails opérationnels.	On fait des revues régulières avec l'équipe sécurité. On identifie les faiblesses mais le traitement prend parfois du temps. Les connexions distantes mal sécurisées et les failles dans les applications anciennes sont problématiques. On essaie de renforcer ces points. Antivirus, VPN, sauvegardes. On a aussi renforcé l'accès physique aux serveurs récemment. La sensibilisation se fait, mais reste ponctuelle. Il faudrait un programme plus structuré.	On utilise des grilles d'évaluation interne, combinées à des résultats de scan de sécurité. Oui, principalement OpenVAS et un outil interne pour la cartographie des vulnérabilités. Ces résultats permettent de revoir nos priorités IT et planifier des mises à jour critiques. Les principales difficultés : les systèmes obsolètes et le manque de temps pour des évaluations approfondies	Non, pas utilisée, mais déjà mentionnée dans des formations. Elle semble complète, mais je ne suis pas sûr qu'elle soit adaptée à notre environnement sans ajustements. C'est une méthode claire, mais trop lourde à déployer en l'état dans notre structure. Pourquoi pas, mais il faudrait l'adapter aux réalités du terrain.

Interview 5 Cadre informatique Niv3 :03ans	Honnêtement, la stratégie est là sur le papier, mais dans la pratique, il y a encore des écarts. L'alignement avec les objectifs métier reste un défi On suit des référentiels, on fait des réunions de coordination, mais parfois ça reste très théorique. Les urgences prennent souvent le dessus. La cybersécurité est intégrée, oui, mais ce n'est pas toujours anticipé dans les projets. On corrige après coup. La direction soutient quand il y a des incidents ou des demandes critiques, mais sinon, elle reste assez distante du quotidien IT.	On a des processus, mais leur efficacité dépend beaucoup de la charge de travail et des priorités du moment. Phishing, logiciels non mis à jour, et aussi les accès non maîtrisés sur certains équipements. La gestion reste manuelle sur certains points. Mots de passe renforcés, double authentification en test, mais pas encore généralisée. Quelques rappels, des mails internes, mais peu de formations formelles ou continues.	Rien de très standardisé. On évalue selon les cas, souvent quand un problème est détecté ou signalé. Quelques outils sont utilisés, mais on n'a pas de cadre bien défini pour tout. Les résultats servent à réagir, pas toujours à prévenir. C'est un axe à améliorer clairement. Manque de temps, manque de ressources, et les systèmes critiques sont difficiles à tester sans risque.	Non, jamais utilisée. J'en ai entendu parler. Peut être utile, mais pas connue ici, donc difficile à appliquer. Trop lourde sans accompagnement. On aurait besoin de formation pour vraiment l'exploiter. Peut-être sur le long terme, si on structure mieux notre approche risques.

Réponse 1 Le RSSI devra avoir plus 15ans d'expérience dont 10ans dan le domaine de sécurité SI	La stratégie globale de gouvernance IT de notre entreprise est centralisée, encadrée par des directives gouvernementales et orientée vers l'intérêt général. L'alignement se fait sur plusieurs niveaux. La gouvernance IT veille à ce que les systèmes améliorent la productivité, réduisent les pertes (fuites, arrêts non planifiés), et optimisent les chaînes d'approvisionnement et de distribution. Principaux éléments de la gouvernance IT appliqués au sein de la DSI sont : -Mise en cohérence des projets IT avec les objectifs métiers et stratégiques de l'entreprise (production, sécurité, transition énergétique). - Travail collaboratif avec les directions métiers pour s'assurer que les besoins sont bien compris, traduits et satisfaits. - Démarche d'amélioration continue (audit, retour d'expérience, benchmarks).	L'efficacité des processus de gestion des risques informatiques est évaluée à travers une approche systématique, combinant référentiels normatifs, audits, Exercices de simulation et tests des plans de réponse, et implication du top management. Défauts de mise à jour et vulnérabilités logicielles Risque : Exploitation de failles non corrigées dans les logiciels métiers ou industriels. Gestion : Gestion centralisée des vulnérabilités Lancement de scanning régulier Tests d'impact avant déploiement de patchs dans les environnements sensibles 1. Sauvegardes isolées et tests réguliers de restauration	via des Scans de vulnérabilités et audits techniques : Audit interne régulier + audit externe en collaboration avec des partenaires spécialisés des Outils de gestion des vulnérabilités (VM - Vulnerability Management), Méthodologie : OWASP Top 10 Les analyses de risques débouchent sur la mise en place ou l'ajustement : Des politiques de sécurité, Des contrôles techniques, Des processus métier (gestion et contrôle d'accès aux systèmes critiques) Limites en ressources humaines et compétences spécialisées	NON Bien adaptée aux entreprises qui cherchent une approche structurée sans coûts de licence. La méthode couvre l'ensemble du cycle : identification des biens, des menaces, des vulnérabilités, des mesures existantes, et des impacts. Mais 0apparait lourde et difficile à déployer sans un appui méthodologique fort, surtout dans des environnements multi-sites ou peu homogènes. Oui, il est pertinent d'inclure MEHARI dans la stratégie de gouvernance IT à long terme.

	La gouvernance IT accorde une place centrale à la gestion des risques cyber, car la sécurité des systèmes d'information est un enjeu stratégique, tant pour la continuité des opérations industrielles que pour la protection des intérêts nationaux. le soutien de la direction générale (DG) est essentiel pour assurer la crédibilité, l'efficacité et la pérennité de la stratégie IT et cybersécurité.	2. Segmentation réseau pour limiter la propagation 3.Plan de réponse à incident (PRI) avec scénario ransomware 4.Sensibilisation des utilisateurs (phishing, pièces jointes piégées) Via des bulletins d'alerte diffusées, lors des réunions, organisation de formation en sécurité informatique		