الجمهورية الجزائرية الديمقراطية الشعبية
People's Democratics Republic of Algeria

Ministry of Higher Education
and Scientific Research

National Higher School of Management
University Pole of Kolea

وزارة التعليم العالي و البحث العلمي

المدرسة الوطنية العليا للمناجمنت
القليعة

MÉMOIRE DE FIN D'ÉTUDES

En vue de l'obtention d'un Master professionnel en
« Gouvernement électronique »

Gestion des Risques Liés à la Sécurité des Systèmes d'Information de la DGI

Elaboré par :

WissaL Bouchra KAID
Doua SALLAH

Encadré par :

Dr. Omar KADI

Année Universitaire : 2025 /2026

RÉSUMÉ

La gestion des risques de la sécurité des systèmes d'information est devenue un critère indispensable pour la continuité effective des activités des institutions gouvernementales. L'objectif de cette étude est de déterminer l'état actuel de la gestion des risques de la sécurité des systèmes d'information au sein de l'administration fiscale algérienne, à travers l'analyse de la Direction Générale des Impôts Nous avons utilisé une méthodologie qualitative basée sur les entretiens semi-directifs avec les employés concernés à la sécurité des SI et une analyse de la méthode d'EBIOS Risk Manager. Les résultats indiquent que la gestion des risques est un élément important dans le cadre de la sécurisation du système d'information, à travers l'identification des vulnérabilités, de la menace et de l'application des mesures de sécurité adaptées. L'absence d'une politique formalisée et documentée de gestion des risques des systèmes d'information au sein de la Direction Générale des Impôts ; les mécanismes existants se limitant à une charte de sécurité générale sans traduction opérationnelle suffisante. En plus le facteur humain est apparu comme la principale source de vulnérabilité, à travers le manque de coordination entre les parties prenantes et l'insuffisance de la communication interne dans la DGI.

Mots-clés : gestion des risques, système d'information, Sécurité des systèmes d'informations, EBIOS RM, vulnérabilité, DGI

ABSTRACT

Information systems Security risk management has become an essential criterion for ensuring the effective continuity of governmental institutions activities. The objective of this study is to determine the current state of information systems Security risk management within the Algerian tax administration, through an analysis of the Directorate General of Taxes (DGI). we used a qualitative methodology based on semi-structured interviews with employees involved in information systems security, as well as an analysis using the EBIOS Risk Manager method. The results indicate that risk management is an important element in securing the information system, through the identification of vulnerabilities and threats and the implementation of appropriate security measures. The study also highlights the absence of a formal and documented information systems risk management policy within the Directorate General of Taxes, with existing mechanisms limited to a general security charter without sufficient operational implementation. Furthermore, the human factor emerged as the main source of vulnerability, due to a lack of coordination between stakeholders and insufficient internal communication within the DGI.

Keywords : Risk management, information system, information systems Security, EBIOS RM, vulnerability, DGI.

ملخص

إدارة مخاطر أمن نظم المعلومات أصبحت معيارًا أساسيًا لضمان الاستمرارية الفعّالة لأنشطة المؤسسات الحكومية. وتهدف هذه الدراسة إلى تحديد الوضع الحالي لإدارة مخاطر أمن نظم المعلومات داخل الإدارة الجبائية الجزائرية، من خلال تحليل حالة المديرية العامة للضرائب. تم استخدام منهجية نوعية تعتمد على مقابلات شبه موجهة مع الموظفين المعنيين بأمن نظم المعلومات، بالإضافة إلى تحليل باستخدام منهجية.EBIOS Risk Manager تشير النتائج إلى أن إدارة المخاطر عنصر مهم في تأمين نظام المعلومات، من خلال تحديد نقاط الضعف والتهديدات وتطبيق إجراءات أمنية مناسبة. كما تُبرز الدراسة غياب سياسة رسمية ومُوثقة لإدارة مخاطر نظم المعلومات داخل المديرية العامة للضرائب، حيث تقتصر الآليات الحالية على ميثاق أمني عام دون ترجمة تشغيلية كافية. بالإضافة إلى ذلك، ظهر العامل البشري كمصدر رئيسي للهشاشة، من خلال ضعف التنسيق بين الأطراف المعنية وعدم كفاية التواصل الداخلي داخل المديرية العامة للضرائب .

الكلمات المفتاحية: إدارة المخاطر، نظام المعلومات، أمن نظم المعلومات، EBIOS RM، الثغرات، المديرية العامة للضرائب

REMERCIEMENTS

Après avoir rendu grâce à Allah, qui m'a permis d'achever ce travail, fruit d'efforts soutenus, de patience et de persévérance, je tiens à exprimer ma profonde reconnaissance à toutes les personnes qui m'ont accompagnée tout au long de ce parcours. Ce travail est le reflet d'un chemin marqué par la détermination, mais aussi par le soutien précieux de ceux qui m'entourent.

J'exprime tout d'abord ma profonde reconnaissance à notre encadreur, Monsieur Kadi Omar, pour son accompagnement, la qualité de ses conseils et son encadrement rigoureux, qui ont grandement contribué à l'aboutissement de ce travail.

Je tiens également à adresser mes remerciements à l'administration de l'établissement pour les moyens mis à notre disposition et pour l'environnement favorable à la réussite de ce projet académique.

J'adresse mes sincères remerciements à ma chère mère, pour son amour inconditionnel, sa tendresse, ses sacrifices silencieux, ainsi que pour ses prières qui ont toujours illuminé mon chemin. Sa présence, sa patience et son soutien constant ont été ma plus grande force dans les moments de doute et de fatigue. Aucun mot ne saurait exprimer pleinement ma gratitude et mon affection envers elle.

J'exprime également ma gratitude à mon père, pour ses conseils avisés et son accompagnement, qui ont contribué à ma réussite.

Mes remerciements vont aussi à mes frères, Amine et Youssef, pour leur présence et leur soutien, ainsi qu'à ma sœur Rajaa, pour sa bienveillance dans les moments délicats. Je remercie également Rachida pour son soutien moral.

Je tiens à exprimer ma profonde gratitude à mon binôme, « ma jumelle de décembre », pour sa patience, sa compréhension, sa complicité et son soutien sans faille tout au long de la réalisation de ce travail.

Je remercie également mes amis et collègues, avec qui j'ai partagé un parcours riche en expériences et en souvenirs.

Mes remerciements s'adressent aussi à Bahaa pour sa contribution et ses encouragements précieux.

Je rends grâce à Allah, conformément à Sa parole : « Certes, les patients recevront leur récompense sans compter ».

Kaid Wissal Bouchra

REMERCIEMENTS

Au début, je remercie Dieu Tout-Puissant qui m'a donné la force et la motivation nécessaires pour accomplir ce travail. Je tiens également à exprimer ma profonde gratitude à mon encadrant kadi Omar pour tous les conseils, le soutien et l'aide qu'il m'a apportés tout au long de cette étude.

J'adresse aussi mes sincères remerciements, mon admiration et ma reconnaissance à celui que je considère comme une source de fierté, mon cher père, professeur et inspirateur, qui s'est sacrifié sans compter pour mon bonheur.

Et à celle qui a été un soutien et un refuge, qui m'a enveloppé de ses prières, qui m'a donné un nom que je porte avec fierté, et qui a quitté ce monde en laissant derrière elle un immense vide, ma chère mère, que Dieu ait son âme et lui accorde Sa miséricorde.
Je remercie également ma famille, qui a été un véritable soutien pour surmonter les difficultés de ce parcours, en particulier la femme de mon oncle, que Dieu la protège et la garde.
Je tiens aussi à remercier mon amie de parcours et compagne de route, « la jumelle de décembre » et partenaire de ce travail, WissaL, qui a été à mes côtés, me soutenant et m'aidant depuis le premier jour d'étude jusqu'aux derniers instants, pour tout ce qu'elle m'a apporté comme soutien moral, motivation et encouragement sous toutes ses formes.
À celles que le destin a réunies avec moi dans la plus belle des rencontres et qui sont devenues des amies de cœur très chères, Hind et Nadine.

Enfin, j'adresse mes remerciements à toute personne, de près ou de loin, ayant contribué à la réalisation de ce travail, ainsi qu'à tous ceux qui m'ont soutenue par un mot bienveillant ou un sourire.

Je dédie ce modeste travail à tous ceux qui ont marqué mon parcours.

Sallah Douaa

Table des Matières

Liste des Tableau

Listes des figures

LISTE DES ABRÉVIATIONS

AD	Active Directory
AGPLv3	Affero General Public License version 3
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
API	Application Programming Interface
APT	Advanced Persistent Threat
CAF	Caisse d'Allocations Familiales
CERT	Computer Emergency Response Team
CLUSIF	Club des Utilisateurs de la Sécurité des Systèmes d'Information
CMMC	Cybersecurity Maturity Model Certification
CRM	Customer Relationship Management
CSF	Cybersecurity Framework
D, I, C, E	Disponibilité, Intégrité, Confidentialité, Évidence
DDoS	Distributed Denial of Service
DGI	Direction Générale des Impôts
DSI	Direction des systèmes d'information
DORA	Digital Operational Resilience Act
EBIOS RM	Expression des Besoins et Identification des Objectifs de Sécurité – Risk Manager
ERP	Enterprise Resource Planning
FISMA	Federal Information Security Management Act
GRC	Gouvernance, Risque et Conformité
IoT	Internet of Things

IRM	Gestion Intégrée des Risques
ISO	International Organization for Standardization
IT	Information Technology
MEHARI	Méthode Harmonisée d'Analyse des Risques Informatiques
NIF	Numéro d'Identification Fiscale
NIS2	Network and Information Security Directive 2
NIST	National Institute of Standards and Technology
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OIDC	OpenID Connect
OT	Operational Technology
OV	Objectifs Visés
PCA	Plan de Continuité d'Activité
PHP	Hypertext Preprocessor
POA&M	Plan of Action and Milestones
RBAC	Role-Based Access Control
RGPD	Règlement Général sur la Protection des Données
RGS	Référentiel Général de Sécurité
RI	Recherche et Intervention
RNSI	Référentiel National de Sécurité de l'Information
RSSI	Responsable de la Sécurité des Systèmes d'Information
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SAN	Storage Area Network

SAP	Systems, Applications, and Products in Data Processing
SEI	Software Engineering Institute
SI	Système d'Information
SIF	Système d'Information Fiscale
SMSI	Système de Management de la Sécurité de l'Information
SR	Source de Risque
SSI	Sécurité des Systèmes d'Information
SSO	Single Sign-On
TIC	Technologies de l'Information et de la Communication
TRM	Threat and Risk Management

INTRODUCTION GÉNÉRALE

1. Contexte de l'étude

À une époque où les données sont devenues extrêmement précieuses et où la gestion numérique est une nécessité plutôt qu'un élément Secondaire, les institutions publiques se retrouvent face à un double défi : assurer l'efficacité numérique sans compromettre la sécurité, et s'ouvrir au monde digital sans exposer les données sensibles à des risques. Aucune institution ne vit cette tension aussi intensément que l'administration fiscale, qui détient dans ses bases de données l'historique financier complet de millions de citoyens et d'entreprises.

La Direction générale des impôts en Algérie se trouve aujourd'hui à un tournant critique. D'une part, elle progresse rapidement vers une numérisation complète de ses services et de ses procédures ; d'autre part, elle fait face à un environnement de menaces en constante évolution, où les sources d'intrusion se diversifient et les méthodes d'attaque deviennent de plus en plus sophistiquées. Entre ces deux dynamiques, apparaît un besoin urgent d'une méthodologie scientifique robuste de gestion des risques, qui ne se limite pas à l'identification des menaces, mais qui permet de les évaluer, de les hiérarchiser et de construire des réponses adaptées à chacune d'entre elles.

2. Objectifs de la recherche

Cette étude vise à atteindre les objectifs suivants :

- Analyser l'état actuel de la gestion des risques liés à la sécurité des systèmes d'information au sein de la DGI.
- Identifier et évaluer les risques affectant le système d'information.
- Examiner le degré d'application de la méthode EBIOS RM.
- Proposer un cadre structuré pour la mise en place de normes et procédures de gestion des risques.
- Promouvoir une culture de sécurité de l'information au sein de l'organisation à travers la sensibilisation du personnel.

3. Problématique d'étude

Pour approfondir ce sujet on propose la question de recherche :

- **Comment la DGI peut-elle structurer une démarche de gestion des risques permettant de renforcer la sécurité de ses systèmes d'information ?**

Cette question principale est complétée par trois (03) sous questions de recherche, à savoir:

- Quel est l'état actuel des dispositifs de gestion des risques liés à la sécurité des systèmes d'information au sein de la DGI, et dans quelle mesure les mesures techniques en place s'inscrivent-elles dans une démarche globale et structurée ?
- Quelle est la méthode d'analyse et de gestion des risques SI la plus adaptée au contexte de la direction générale des impôts ?
- Dans quelle mesure le facteur humain à travers les comportements des utilisateurs, la faiblesse de la coordination inter-parties prenantes et l'insuffisance de la sensibilisation aux cybermenaces constitue-t-il le principal vecteur de vulnérabilité au sein du SI de la DGI ?

4. Pertinence de la recherche

Cette étude présente une pertinence théorique en contribuant au développement des connaissances dans le domaine de la gestion des risques liés à la sécurité des systèmes d'information au sein de la Direction Générale des Impôts. Elle propose également des processus pratiques et applicables visant à améliorer le niveau de sécurité de l'information, ce qui en fait une étude à la fois pertinente sur les plans théorique et managérial.

4.1. Pertinence théorique

Cette recherche s'inscrit dans le domaine de la gestion des risques liés à la sécurité des systèmes d'information et vise à enrichir le cadre théorique de plusieurs manières :

- En élargissant la compréhension des processus de gestion des risques liés à la sécurité des systèmes d'information et des méthodes utilisées pour en assurer l'efficacité.
- En analysant l'application d'une méthodologie (telle que EBIOS RM) dans le contexte d'une institution publique comme la Direction Générale des Impôts.
- En mettant en évidence le rôle de la gouvernance de la sécurité dans la réduction des menaces cybernétiques et le renforcement de la protection des actifs informationnels.

4.2. Pertinence managériale

La problématique de recherche présente une pertinence directe pour les responsables et les praticiens de la sécurité des systèmes d'information au sein de la Direction Générale des Impôts, en ce qu'elle contribue à :

- Proposer un cadre pratique pour améliorer la gestion des risques liés à la sécurité des systèmes d'information au sein de la direction.
- Aider les décideurs à mieux comprendre les vulnérabilités et les menaces susceptibles d'affecter le système d'information.
- Soutenir la prise de décisions efficaces visant à renforcer les contrôles de sécurité et à réduire les risques cybernétiques.
- Permettre à l'institution d'adopter les meilleures pratiques en matière de sécurité de l'information afin d'assurer la continuité des services et la protection des données sensibles.

5. Choix de l'Entreprise

Notre étude a été réalisée au sein de la Direction Générale des Impôts (DGI), et ce choix repose sur plusieurs considérations essentielles. Tout d'abord, cette institution figure parmi les principales entités publiques jouant un rôle central dans la gestion des ressources fiscales de l'État, ce qui lui confère une importance stratégique majeure.

Deuxièmement, la Direction a connu ces dernières années une orientation marquée vers la numérisation et la modernisation de ses systèmes d'information, notamment en matière de renforcement de leur sécurité et de gestion des risques associés, ce qui en fait un terrain pertinent pour étudier l'efficacité de ces efforts.

Troisièmement, en tant qu'acteur clé évoluant dans un environnement administratif complexe et sensible, la Direction Générale des Impôts offre un cadre riche pour comprendre les enjeux liés à la gouvernance et à la sécurité des systèmes d'information au sein des institutions publiques.

Quatrièmement, le domaine fiscal est rarement abordé sous l'angle de la gestion des risques liés à la sécurité des systèmes d'information, ce qui rend l'étude de ce sujet au sein de la Direction Générale des Impôts particulièrement pertinente et nécessaire à l'heure actuelle.

6. Raisons du choix du thème

Le choix du thème **« La gestion des risques liés à la sécurité des systèmes d'information selon la méthode EBIOS RM au sein de la Direction Générale des Impôts »** se justifie par plusieurs raisons :

- Il s’agit d’un sujet d’actualité qui s’impose avec la transformation numérique des administrations publiques.
- L’augmentation des cyber-risques qui menacent les systèmes d’information, notamment dans les institutions traitant des données sensibles comme la DGI.
- La nécessité de mettre en évidence le rôle de la gestion des risques dans l’anticipation et la prévention des menaces informatiques.
- Le manque d’études appliquées dans le contexte de l’administration fiscale algérienne, ce qui renforce la pertinence et l’originalité de ce travail de recherche.

7. La méthodologie utilisée

Pour examiner l’efficacité de la gestion des risques liés à la sécurité des systèmes d'information au sein de la Direction Générale des Impôts, notre étude adopte une méthodologie qualitative fondée sur les étapes de la méthode EBIOS Risk Manager (EBIOS RM), qui permet d’analyser et d’évaluer les risques de manière structurée et rigoureuse.

Cette méthodologie repose sur la collecte de données qualitatives à travers des entretiens semi-directif aux employés et cadres concernés par la sécurité des systèmes d'information, ainsi que sur l’analyse des données relatives aux menaces, aux vulnérabilités et aux actifs informationnels sensibles. Elle inclut également l’identification de scénarios de risques selon les étapes de la méthode EBIOS RM, notamment en ce qui concerne l’étude des sources de menace et des événements redoutés.

L’étude s’appuie par ailleurs sur l’évaluation des risques à travers la mesure de la probabilité d’occurrence des menaces et de leur impact sur le système d'information, en utilisant des indicateurs quantitatifs pour estimer le niveau de criticité. Des indicateurs liés à l’efficacité des contrôles de sécurité mis en place sont également calculés afin d’évaluer leur capacité à réduire le niveau de risque.

À travers cette approche qualitative, nous visons à fournir une analyse objective et précise du niveau de maturité de la gestion des risques liés à la sécurité des systèmes d'information, à identifier les points forts et les faiblesses, et à proposer des améliorations concrètes pour renforcer la sécurité du système d'information et assurer la continuité des services.

8. Structure du mémoire

Notre mémoire sera organisé en trois chapitres distincts afin de traiter efficacement notre problématique. Dans un premier temps, nous exposerons notre démarche de recherche en présentant le contexte et la problématique de manière détaillée dans la partie Introduction générale de notre mémoire, en justifiant le choix du thème, les objectifs de la recherche ainsi que la méthodologie adoptée.

Le premier chapitre sera consacré à une revue de littérature portant sur la gestion des risques liés à la sécurité des systèmes d'information, à travers l'exploration d'une sélection d'articles et de travaux académiques pertinents. Ensuite, dans la deuxième section, nous aborderons le cadre conceptuel, où nous fournirons des éclaircissements et des informations pertinentes pour mieux appréhender notre sujet de recherche, notamment les notions fondamentales d'actif, de menace et de vulnérabilité. La troisième section présentera un résumé des différentes méthodes d'analyse des risques, notamment EBIOS RM, MEHARI et OCTAVE, ainsi que les critères qui ont guidé le choix de la méthode la plus adaptée au contexte de la Direction Générale des Impôts.

Le deuxième chapitre se concentrera sur le cadre méthodologique et le contexte organisationnel de notre étude. Ce chapitre sera également divisé en deux parties. La première section sera consacrée à la présentation de la Direction Générale des Impôts, de sa structure organisationnelle et des fonctions de la sous-direction de la gouvernance et de la sécurité des systèmes d'information fiscale. La deuxième section décrira l'approche méthodologique qualitative adoptée, en détaillant les étapes et les méthodes utilisées pour recueillir et analyser les données à travers des entretiens semi-directifs, des observations et une analyse documentaire approfondie.

Le troisième chapitre, intitulé « Résultats et Discussions », sera dédié à l'analyse et à la discussion des résultats obtenus. Il comprendra une simulation de la mise en œuvre de la méthode EBIOS Risk Manager appliquée au portail fiscal Jibaya'tic, structurée en cinq ateliers successifs allant du cadrage et du socle de sécurité jusqu'au traitement des risques. Ce chapitre présentera également les résultats des entretiens, leur analyse thématique et leur mise en perspective avec la littérature existante.

Enfin, notre travail se conclura par une synthèse dans laquelle nous résumerons l'ensemble de nos résultats et tenterons de répondre à notre problématique initiale, tout en formulant des recommandations pratiques et en ouvrant des perspectives pour de futures recherches dans le domaine de la cybersécurité des administrations fiscales publiques algériennes.

CHAPITRE I

REVUE DE LITTÉRATURE ET CADRE CONCEPTUEL

Les transformations numériques dans l'environnement institutionnel, plus précisément dans l'administration publique, ont accentué l'importance stratégique de ces systèmes dans le fonctionnement et le rendement des institutions. Ces derniers sont devenus essentiels pour la gestion et le traitement des données mais, au même moment, font face à une variété de risques d'un point de vue de leur sécurité, de leur fiabilité et de la continuité de leurs services. En conséquence, il faut faire une attention particulière à la gestion des risques dans les systèmes d'information, spécialement au sein de l'administration publique utilisant une grande quantité de données sensibles, par exemple, liées à l'impôt. De nombreuses recherches ont porté sur la sécurité du système informatique et sur la gestion des risques. Il a été mis en évidence l'importance de l'établissement des normes, référentiels et mécanismes de contrôle interne. Par conséquent, il est nécessaire d'examiner le fondement théorique tirées de diverses recherches liées à la thématique des systèmes d'information à leur sécurité et à la gestion des risques. La nécessité est d'identifier également les lacunes des recherches précédentes, parmi lesquelles on peut citer leur faible application dans l'administration publique fiscale. C'est ce que nous aborderons dans ce chapitre.

Section 01 : Revue de littérature

Les recherches passées ont traité de l'importance du système d'information dans les institutions administratives, en précisant le rôle de la gestion des risques liés à la sécurité du système d'information pour la protection des données et la continuité du service public. Elles ont insisté que la mise en place de procédures efficaces de gestion des risques contribue à réduire les incidents et à faire face aux menaces.

1. Sécurité des systèmes d'information

Plusieurs études montrent que les chercheurs n'ont pas la même vision lorsqu'il s'agit de définir le système d'information D'après MAHRRAR Amina et KERZABI Abdelatif 2021 Dans leurs article intitulé « Le système d'information en Algérie : un saut compétitif pour les entreprises algériennes » Le système d'information englobe l'intégralité des flux informationnels au sein de l'organisation, avec les ressources humaines et techniques mobilisées pour garantir leur suivi et leur traitement (MAHRRAR & KERZABI, 2021)

Et selon RDJAM Khaled, BEN AMMARA Taher et DHOUAR Mohamed Yazid 2018 de l'article « Évaluation de la performance du système d'information électronique : étude comparative entre l'Office National de la Météorologie et l'entreprise HESS », " le système d'information est un point de vue technique, comme un ensemble de composantes interconnectées visant à collecter, traiter, stocker et diffuser l'information afin de soutenir la prise de décision et le contrôle au sein de l'organisation. Les systèmes d'information aident également la direction à analyser les problèmes en fournissant l'information appropriée au moment opportun ". (Khaled, BEN AMMARA , & DHOUAR, 2018)

D'après la Thèse de Doctorat intitulé « Atla Sec, Une approche pour la maitrise de la Sécurité de l'information adaptée aux systèmes de systèmes » écrit par RABII Anas 2023, ce n'est pas le manque de standards de sécurité qui est le véritable problème, mais bien la façon de les mettre en œuvre dans un système complexe. Cela implique donc qu'une stratégie d'ensemble basée sur la modélisation doit être utilisée pour la gestion du risque Il considère que l'accroissement de la complexité des systèmes d'information a rendu difficile l'application des solutions de sécurité et la correction des vulnérabilités. Il a ainsi proposé l'adoption d'une nouvelle méthodologie de gestion de la sécurité de l'information dans les systèmes caractérisés par leur complexité, à savoir la méthodologie Atla Sec L'étude a démontré sa capacité à améliorer la compréhension des risques de sécurité, à faciliter

l'analyse des menaces et leur lien avec les actifs, ainsi qu'à optimiser le choix des solutions de sécurité et à réduire les risques de manière significative (RABII, 2023).

Selon un article de MEKIMAH Sabri et ZERDOUDI Amina 2022 intitulé « L'évaluation du système de management de la sécurité de l'information (SMSI) Aux normes internationales iso 27001 : Étude de cas de l'entreprise portuaire de Skikda. -Algérie- », ils estiment qu'il est nécessaire d'adopter sérieusement un système de sécurité de l'information afin de fournir aux acteurs les compétences requises pour réaliser des audits internes, garantissant ainsi l'amélioration continue de la sécurité du système d'information et sa conformité aux exigences de la norme internationale Cette étude a établi que le respect de la mise en œuvre des normes de sécurité du système informatique se fait d'une manière satisfaisante parmi les établissements algériens. Cela nécessite qu'il soit important d'établir un respect strict de toutes les exigences réglementaires de ces normes ainsi que des exigences d'audit interne afin d'améliorer la mise en œuvre des normes ISO 27001 (Sabr & ZERDOUDI , 2022).

En ce qui concerne Référentiel National de Sécurité de l'Information telle que déterminée par Ministère de la Poste, des Télécommunications (MPT)2020, qui sert à mettre en place un cadre de sécurité de systèmes d'information au niveau national qui harmonise les politiques et procédures de sécurité des systèmes d'information dans un environnement de risques croissants, la sécurité de systèmes d'information du secteur public est considérée comme requérant un cadre national unique basé sur l'identification des risques, leur évaluation et leurs solutions. Il en a résulté l'élaboration d'un cadre global pour la gestion de la sécurité de l'information ainsi que la mise en place d'une méthode globale de gestion des risques pour protéger la confidentialité et l'intégrité des informations, mais aussi pour attribuer les rôles et responsabilités dans les organisations, en se rappelant que la sécurité de l'information est un effort collectif nécessitant une intervention technique et juridique rigoureuse (Ministère de la Poste, des Télécommunications, 2020) .

L'article intitulé « ENSURING INFORMATION SECURITY IN PUBLIC ORGANIZATIONS IN THE REPUBLIC OF MOLDOVA THROUGH THE ISO 27001 STANDARD » de Arina Alexei 2021 portait sur l'évaluation du niveau de conformité des contrôles nationaux de la Moldovie à l'état international en ce qui concerne la sécurité de l'information. Cette auteure affirme qu'il est essentiel de veiller à une conformité adéquate aux normes internationales et une protection adéquate des informations pour la création de la confiance en la sécurité de l'information L'étude a montré qu'il existait un désaccord concernant les normes nationales et internationales, mais aussi qu'il était nécessaire de

consolider la confiance et de garantir la sécurité lors du partage d'informations. (Alexei, 2021)

D'après RDJAM Khaled, BEN AMMARA Taher et DHOUAR Mohamed Yazid 2018 de l'article « Évaluation de l'efficacité du système d'information électronique : étude comparative entre l'Entreprise nationale de géophysique et l'entreprise partenaire HESS (étrangère – Sonatrach) », il y a plusieurs problèmes concernant le développement des systèmes d'information et la garantie de leur sécurité. En effet, la question ne touche pas uniquement le domaine technologique. Les ressources doivent être correctement gérées et utilisées pour obtenir un avantage sur le marché. Selon l'étude, l'inadéquation entre les ressources et le manque de contrôle peuvent entrainer un système non efficace alors que l'efficacité des systèmes et une bonne utilisation des ressources contribueront à la création d'un système d'information sécurisé (Khaled, BEN AMMARA , & DHOUAR, 2018).

Selon MAHRRAR Amina et KERZABI Abdelatif 2021 dans leur article intitulé « Le système d'information en Algérie : un saut compétitif pour les entreprises algériennes », le système d'information constitue un facteur stratégique essentiel pour la réussite des institutions algériennes. Il est donc nécessaire de relever les défis qui y sont associés et de surmonter les difficultés et obstacles entravant la mise en œuvre d'une approche globale de la sécurité des systèmes d'information, en soulignant que cette sécurité est devenue une nécessité incontournable dans le contexte actuel de la transformation numérique (MAHRRAR & KERZABI, 2021).

2. Gestion des risques

Dans leur article (Mohamed & Ahmed Gaid , 2017), « Contribution de l'audit interne dans la gestion des risques liés aux systèmes d'information dans le cadre de la gouvernance des systèmes d'information - Cas Evol Ute c International – Algérie »**,** a défini les risques comme étant le potentiel d'une occurrence qui influera sur l'efficacité d'une organisation dans l'atteinte de ses objectifs. Selon leur nature, ces risques pourraient inclure techniques, tels que les pannes technologiques ; Humains, par exemple, les erreurs des utilisateurs ; Ou extérieurs, par exemple, virus informatiques et attaques cybernétiques. Les conséquences de ces risques se traduisent par des menaces portant sur les actifs de l'organisation, perturberont les opérations quotidiennes Ils estiment que la gestion et le contrôle des risques par l'intermédiaire de l'audit interne constituent un facteur d'une importance doublement cruciale.

Dans son article « LES RISQUES LIES AUX T.I.C DANS L'ENTREPRISE : Essai d'analyse à partir échantillon d'entreprises algériennes. », ARBAOUI Khaira considère que les risques sont en fait causés par un usage incorrect des technologies de l'information et de la communication (TIC) Elles se divisent en : risques technologiques, organisationnels, stratégiques et risques économiques des connaissances issues de l'utilisation incorrecte de la technologie, de la formation incomplète et de l'absence d'intégration entre l'innovation, l'éducation et les institutions. Il met l'accent sur l'importance de l'usage correct des TIC pour limiter ces risques, alors que l'utilisation incorrecte est un risque réel (KHEIRA, 2012).

Selon l'article « Le contrôle interne : dispositif permanent et indispensable pour la maitrise des risques liées aux systèmes d'information » par BOUYAHIAOUI Adel, DAHIA Abdelhafidh 2022, le principal risque est lié aux défauts du contrôle interne de l'institution. Risque d'informations peut se réaliser par leur fuite, perte totale d'information et panne des systèmes. Dans ce cas, l'information sera susceptible d'être détruite, illégitimement accédée et moins fiable, entraînant donc une baisse de productivité de l'entreprise, ainsi que la menace pour sa survie. Cependant, une bonne interne permettra non seulement de minimiser les risques de sécurité de l'information, mais aussi d'améliorer la qualité de cette information (Adel & DAHIA , 2022) .

3. Gestion des risques en sécurité de si

À travers la revue de la littérature et l'examen des différents articles liés au sujet de notre étude, nous avons constaté l'existence de certaines lacunes de recherche qui n'ont pas été abordées dans les travaux antérieurs consultés. Elles peuvent être présentées comme suit :

L'ensemble des articles étudiés (KHEIRA, 2012) , (MAHRRAR & KERZABI, 2021) , (Mohamed & Ahmed Gaid , 2017)**,** n'a pas appliqué leur analyse théorique aux institutions fiscales publiques, se limitant plutôt aux entreprises privées. Ainsi, notre étude propose une application du thème de la gestion des risques et de la sécurité des systèmes d'information au niveau de la Direction Générale des Impôts.

Selon (Adel & DAHIA , 2022)Le système fiscal algérien rencontre des difficultés dans la mise en place d'un cadre unifié et global concernant la gestion des risques menaçant la sécurité de son système d'information, notamment en matière de protection des données fiscales des contribuables et de modernisation des systèmes existants. Par ailleurs, en ce qui concerne la DGI, il n'existe pas d'étude précise et structurée traitant spécifiquement de la gestion des risques.

On observe également une faiblesse du taux d'application des normes dans les institutions publiques algériennes. D'après une étude donnée, le taux moyen de conformité à la norme dans l'institution étudiée ne dépasse pas 67,14 %, ce qui indique une certaine avancée vers l'application de la norme, mais reste insuffisant en termes d'efficacité et de performance dans l'article (MAHRRAR & KERZABI, 2021).

Bien que la Direction générale des impôts (DGI) connaisse une phase de transformation numérique accélérée, elle a concentré ses efforts sur l'aspect matériel et tangible de la gestion des risques, sans prendre en compte les risques spécifiques aux systèmes fiscaux numériques, tels que la déclaration électronique, le paiement en ligne et l'échange de données avec d'autres administrations. La thèse Atla Sec (RABII, 2023)montre que la complexité des systèmes de systèmes, couplée à l'absence d'outils pour leur mise en œuvre pratique, accroît la difficulté d'aboutir à une méthodologie précise de gestion des risques. La DGI en est un exemple, car elle constitue un système complexe qui intègre plusieurs directions régionales, des plateformes numériques et des bases de données fiscales interconnectées, ce qui la rend vulnérable à des scénarios non traités.

Les études actuelles sur la gestion des risques des systèmes d'information en Algérie montrent qu'elles se concentrent essentiellement, soit sur les entreprises privées de manière plus large, soit sur des cas génériques, en s'appuyant sur des référentiels tels que la norme ISO, mais avec un niveau d'application insuffisant. Elles ne tiennent pas compte de la spécificité de l'administration fiscale publique, représentée par la DGI, qui connaît une transformation numérique continue et fait face à des défis liés à la confidentialité des informations et à sa structure organisationnelle. Cela donne lieu à l'émergence de risques qui n'ont encore été ni étudiés ni encadrés.

Section02 : cadre conceptuel de recherche

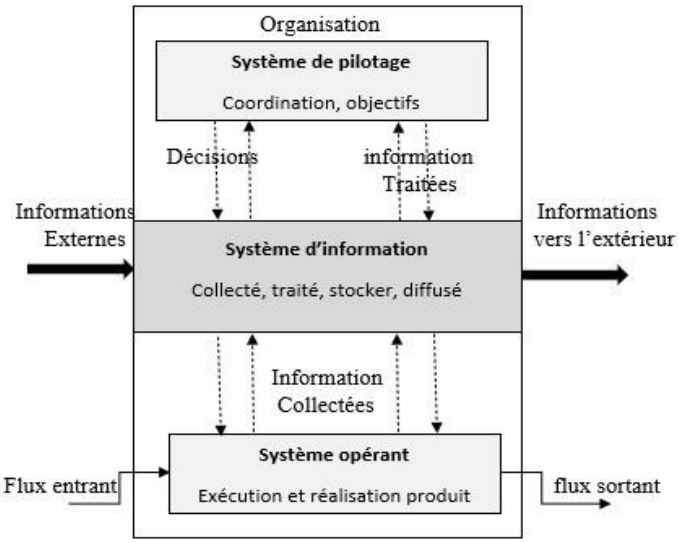
4. Système d'information

4.1. Définition

Selon (laudon & jane, 2017) définissent le système d'information comme suit : " est un ensemble de composantes interreliées qui recueillent de l'information, la traitent, la stockent et la diffusent afin d'aider à la prise de décision, a la coordination et au contrôle au sein d'une organisation. "

L'organisation peut se décomposer en 3 sous-systèmes : Le système de pilotage (appelé également système de décision) le système d'information et Le système opérant :

Figure 1: modèle systémique de l'organisation.



Source : (varinard, 2018)

a. Système de pilotage

Le système de pilotage se situe au sommet de la hiérarchie organisationnelle. Il fonctionne en cohérence avec les objectifs et les politiques de l'organisation. Ce système exploite les informations circulant au sein de l'organisation afin d'orienter, de coordonner et de contrôler le fonctionnement global. Il joue également un rôle essentiel dans la prise de décision et dans la définition des actions à mettre en œuvre au niveau du système opérationnel.

b. Système d'information

- Le système d'information (SI) occupe un rôle crucial dans la collecte, le traitement, le stockage et la diffusion de l'information (données, textes, images, sons, etc.) au sein et entre les organisations.
- Le système d'information peut être considéré comme l'élément qui assure la liaison entre les deux systèmes, en fournissant et en orientant les informations nécessaires à la prise de décision.

c. Système opérant

- Le système opérationnel exécute les tâches qui lui sont attribuées. Il génère également des informations qu'il transmet au système de pilotage afin de faciliter le suivi des écarts et la mise en œuvre des actions nécessaires
- Il englobe toutes les fonctions relatives aux opérations spécifiques de l'entreprise, telles que la facturation des clients, le versement des salaires et la gestion des stocks.

4.2. Importance des systèmes d'information dans l'administration publique

- Il joue un rôle central dans la collecte, le traitement et l'utilisation des données fiscales. Recueillir et intégrer les informations Il rassemble les données de diverses provenances, qu'elles soient internes (déclarations des contribuables, suivi des paiements) ou externes (banques, autres administrations), puis il les structure et automatise leur traitement. Cela rend les informations plus facilement accessibles pour les divers services fiscaux et rend leur travail plus efficace.
- Support à la décision L'information seule ne décide pas, mais elle est un outil précieux entre les mains des responsables fiscaux, Elle favorise une meilleure compréhension des situations des contribuables, la détection des irrégularités et la définition d'actions ciblées pour le recouvrement et la conformité fiscale.
- Apprentissage organisationnelles systèmes d'information permettent aux services fiscaux d'identifier plus précisément leurs besoins et d'adapter leurs objectifs. Ils permettent de comprendre les tendances de recouvrement, de prévoir les risques fiscaux et d'optimiser les procédures.
- Transformation organisationnelle La mise en place d'un système d'information moderne change les modes de travail au sein de l'administration fiscale, améliore la coordination entre services et peut conduire à réviser certaines missions ou responsabilités.
- Gestion du conflit et du pouvoir Le contrôle et le flux d'informations influencent les relations entre les différents services fiscaux. Bien employé, le système est susceptible d'équilibrer l'accès aux informations stratégiques ; employé de manière inappropriée, il peut renforcer les disparités de pouvoir.
- Transparence et raisonnement En rendant l'information plus claire et plus accessible, le système favorise la transparence des opérations fiscales et une meilleure rationalité

dans les décisions. Son importance dépend toutefois des pratiques et des choix des gestionnaires.

Pour résumer, le système d'information n'est pas qu'un outil technique : il organise les données fiscales, appuie la décision, favorise l'apprentissage des services, transforme les pratiques et influence la gestion du pouvoir et de l'information au sein de l'administration.

4.3. Sécurité des systèmes d'information

La sécurité des systèmes d'information définie par (CLUSIF, 2025, p. 15) comme l'étude des vulnérabilités pouvant affecter un système, afin de définir et de déployer des mesures organisationnelles et techniques assurant un niveau de service acceptable. Elle repose sur quatre critères essentiels : la disponibilité, l'intégrité, la confidentialité et la traçabilité.

4.3.1. La sécurité informatique

4.3.1.1. Définition

La sécurité informatique regroupe l'ensemble des moyens humains, techniques et organisationnels mis en œuvre pour prévenir, limiter et réparer les risques liés aux systèmes d'information (felidj, miguel, & virginie , 2021, p. 293).

4.3.1.2. Les objectifs de la sécurité informatique

La sécurité informatique a pour vocation d'assurer le maintien, à un niveau approprié, les garanties suivantes : (felidj, miguel, & virginie , 2021, pp. 293-294)

- **L'intégrité**

Les données doivent exister en une version unique et authentique au sein de l'entreprise. Toutes les mesures nécessaires doivent être prises pour empêcher leur altération, leur suppression ou leur duplication non autorisée.

- **La disponibilité**

Toute action ou transaction doit obtenir une réponse immédiate. Les applications doivent pouvoir être utilisées sans délai d'attente, et les requêtes s'exécuter sans temps de latence.

- **La confidentialité**

Les données ne doivent être accessibles qu'aux personnes qui en sont les destinataires ou les propriétaires légitimes.

- **La preuve**

Souvent désignée par les notions de traçabilité, d'imputabilité et de non-répudiation, la preuve garantit qu'il est possible d'identifier avec certitude l'auteur de toute action effectuée sur le système.

4.4. Définitions des concepts de base

4.4.1. Notions fondamentales : Actif, Menace et Vulnérabilité

Les trois notions d'actif, de menace et de vulnérabilité forment le triptyque fondamental de toute démarche de gestion des risques en sécurité de l'information, et méritent à ce titre d'être définies avec précision.

4.4.1.1. Définition “ actif “

Selon la norme ISO 27005 (pons, 2022)un actif est défini comme “tout ce qui a de la valeur pour l’organisation et donc nécessite d’être protégé “, et est divisé en deux catégories :

- **Actifs primaires :** constituent l'élément central de l'organisation. Ils comprennent à la fois les processus métier et les informations dont dépend la mission de l'entreprise.
- **Actifs support :** englobe le matériel, les réseaux, les logiciels, le personnel, les sites ainsi que les structures organisationnelles.

4.4.1.2. Définition “ menace “

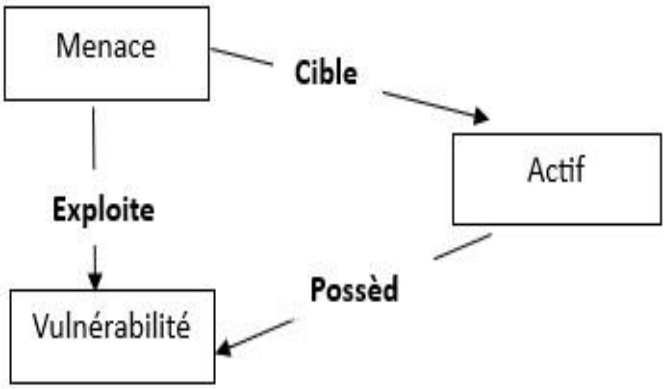
Selon la norme ISO 27001 (lupfer, 2010, pp. 21 - 22) une menace est définie comme “cause potentielle d’un incident indésirable, qui peut nuire à un système ou un organisme “. La norme ISO/IEC 27005 indique qu'une menace doit être définie par certains éléments fondamentaux :

- **Le type :** il aide à classifier les menaces
- **La nature :** elle apporte des précisions sur le degré de contrôle de la menace.
- **L'origine de la menace :** elle porte sur le repérage et le tri des agents créant la menace.
- **La motivation :** liée à la source de la menace, aide a prise des décisions

4.4.1.3. Définition “ vulnérabilité “

Conformément à la norme ISO/IEC27001 (lupfer, 2010, p. 24) une vulnérabilité se définit comme “faille dans un actifs ou dans une mesure de sécurité qui peux être exploitée par une menace. “

Figure 2 : Représentation graphique de trio (actif, menace, vulnérabilité).



Source : (lupfer, 2010)

5. Définition du risque

Selon iso 31000 (INTERNATIONAL ISO31000, 2018)“ l'effet de l'incertitude sur les objectifs“

- **La mesure du risque**

Risque = Menace × Impact × Vulnérabilité

5.1. Les typologies de risques Les risques peuvent relever :

- **De l’humain** : Les risques humains résultent principalement d'un manque de compétences ou de formation insuffisante. Ils peuvent également découler de l'absence de personnel clé, d'un désengagement des utilisateurs, de comportements malveillants internes, ou encore de défaillances dans le dispositif de contrôle interne
- **De la technique :** Les risques techniques sont inhérents à l'évolution technologique et peuvent se manifester sous forme de pannes matérielles, de dysfonctionnements des dispositifs de sécurité, ou d'incompatibilités liées à l'intégration de nouvelles solutions.

- **De l'organisation :** Parfois, le risque est créé par les utilisateurs eux-mêmes, par incompétence ou par hostilité. Parfois, il s'agit d'un manque de procédures… ou au contraire de procédures trop lourdes et complexes.
- **De la planification** : Si les délais sont trop courts ou les budgets trop serrés, le projet est condamné dès le départ. Le résultat est un cruel manque d'agilité.
- **Des contrats :** Un contrat trop rigide finit par tout bloquer – on appelle ça un effet sclérosant.
- **Du domaine managérial :** Les risques managériaux sont liés à la définition d'objectifs peu réalistes, à l'insuffisance des ressources humaines mobilisées, à une gouvernance défaillante et à l'absence de mécanismes d'alerte permettant de détecter les dérives en temps opportun.
- **Du domaine financier** : Là, les risques les plus fréquents sont les corrections de trajectoire non prévues au budget et les mauvaises anticipations.
- **Des partenaires** (clients, fournisseurs, sous-traitants) : Ce qui arrive le plus souvent, c'est soit un partenaire qui défaillit, soit un client mécontent, soit une rupture brutale du contrat.
- **Du marché :** L'apparition d'un nouvel entrant ou une chute brutale des prix sont autant d'événements possibles.
- **Des produits ou services :** Ils peuvent être incomplets, défectueux ou non conformes à la commande, notamment si les besoins ont été mal exprimés.

6. Risque en sécurité des si

La sécurité des systèmes d'information constitue un enjeu stratégique majeur pour les organisations, d'où la nécessité de définir avec précision la notion de risque en sécurité des systèmes d'information qui en est le fondement.

6.1. Définition

D'après la norme ISO/IEC 27005**,** (pons, 2022, pp. 30 - 31) **"** Le risque est la possibilité qu'une menace cible un actif, en exploitant une de ses vulnérabilités et entraînant des conséquences non désirées pouvant avoir un effet sur l'organisation. "

Selon La norme ISO 27001 (jugier, 2021) "Le risque de sécurité de l'information est associé à la possibilité que des menaces exploitent les vulnérabilités d'une ressource informationnelle et causent ainsi un préjudice à un organisme"

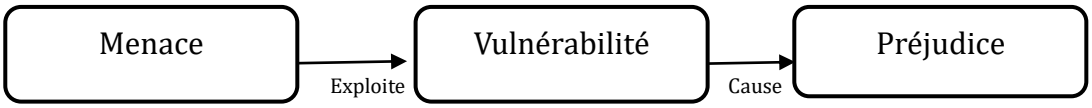
Selon la Référentiel National de Sécurité de l'Information ((MPT), 2020, p. 89) "Exposition à un danger, à un préjudice ou à une perte pouvant être rencontrés lorsqu'une vulnérabilité est exploitée par une menace. Le niveau d'impact sur les services de l'entité, les actifs informationnels ou les individus est le résultat des conséquences potentielles d'une menace et la probabilité que cette menace se produise. "

Donc Le risque de sécurité des systèmes d'information correspond à la probabilité qu'une menace mette à profit une vulnérabilité d'un actif informationnel, et cause ainsi des dommages ou des pertes à l'organisation.

Probabilité=menace*vulnérabilité
Risque=probabilité*conséquence

Source : iso 27005 (pons, 2022, p. 36)

Figure 3: définition des risques en si.



Si Pas de menace ; donc le risque =0

Si Pas de vulnérabilité ; donc le risque =0

Source : préparer par nous même

6.2. La typologie des risques

Les risques peuvent être classés en fonction de leur nature : physique, logique (malware), humain. (felidj, miguel, & virginie , 2021)

6.2.1. Risques Physiques

- **Les pannes** correspondent aux arrêts de machines et de périphériques, avec leur conséquence se manifestant sous forme de diminution de la productivité associée.
- **Les accidents** comprennent des incidents comme une tasse de café tombée sur un ordinateur portable, des dégâts des eaux et des chutes de matériel.

- **Un incident** peut être météorologique (orage et foudre capables de détruire une box, inondation, chaleur capable de fondre des disques) ou non (incendie, surtension). Ils peuvent endommager le matériel.
- **Une attaque par déni de service (DDoS) :** implique d'envoyer un volume massif de requêtes vers une cible précise, comme un serveur, pour le saturer. Noyée sous cet afflux de demandes, la machine devient incapable de traiter les requêtes normales et finit par ne plus répondre.

6.2.2. Risque Logique (Malware/Logiciel) :

- **Un ver :** est un code malveillant indépendant se multipliant par l'intermédiaire de la messagerie et du réseau.
- **La bombe :** est un virus qui, après une infection, demeure silencieux et se lance à un certain moment ou lors de la réalisation de certaines actions. Si des millions de machines ou d'objets connectés sont infectés et lancent leurs programmes simultanément, ils peuvent déstabiliser un réseau ou Internet.
- **Le cheval de Troie :** est un virus apparaissant sous forme de programme légitime (jeu, utilitaire), qui contient un élément malveillant, donnant la possibilité de retourner des informations, d'effectuer un enregistrement de frappes ou de créer une porte d'entrée pour un autre virus.
- **Le rogue** (ou scareware) : est un logiciel (ou une page web infectée) affirmant détecter un virus et promettant sa désinfection. L'exécution du logiciel ou la désinfection en ligne aboutit, au contraire, à son installation.
- **Le spam :** représente le courrier indésirable non sollicité. Il est dangereux car il engendre une perte de temps pour l'utilisateur qui le lit ou le supprime lui-même, surcharge les serveurs de messagerie et consomme de la bande passante.
- **Le phishing**, étant d'abord un spam, imite graphiquement un message provenant d'une organisation connue des utilisateurs (banque, CAF, impôts, etc.). Le message est attrayant et incite à se connecter pour régler un problème. Le site est identique à l'original, mais toutes les données entrées sont récupérées par l'attaquant.
- **Le ransomware** est l'un des dangers actuels. C'est un virus qui a pour but de rendre l'ordinateur inutilisable (écran bloqué, affichage d'un message interdisant tout travail,

chiffrement de fichiers). Une fois la machine infectée, une rançon est demandée à la victime (généralement en cryptomonnaie).

- **Le keylogger** est un enregistreur de frappes, qui enregistre toutes les actions effectuées au clavier (sites visités, mots de passe, etc.).
- **Les logiciels espions** (spyware) sont analogues à des agences d'espionnage et leur but est de transmettre certaines informations à un tiers.
- **Les exploit kits** sont des petites boîtes à outils permettant à un attaquant d'exploiter automatiquement des vulnérabilités connues dans des logiciels, afin de compromettre un système.

6.2.3. Risque humain

- **L'ingénierie social :** consiste à manipuler une victime en exploitant Internet l'attaquant commence par collecter des informations personnelles disponibles en ligne (lieu de résidence, relations, centres d'intérêt) afin de gagner la confiance de sa cible.
- **Le hoax** : est un canular visant à collecter des adresses électroniques ou à pousser les utilisateurs à boycotter une marque.
- **La fraude au président** repose sur l'ingénierie sociale : l'attaquant se fait passer pour le dirigeant de l'entreprise afin de demander par email un virement bancaire urgent et confidentiel.
- **L'APT (Menace Persistante Avancée)** est une combinaison de différentes techniques et outils permettant de s'introduire discrètement dans un réseau, en prenant tout le temps nécessaire (de quelques mois à plusieurs années).
- **Erreurs et mises à jour :** Les erreurs de configuration constituent une menace sérieuse, notamment l'oubli de modification du mot de passe par défaut ou un mauvais choix dans les paramètres de sécurité. Le manque de mises à jour représente un risque majeur, permettant à des failles datant de plus de 10 ans de compromettre des serveurs ou des smartphones.
- **Vol, divulgation, suppression et altération :** Le vol de matériel ou de données ainsi que la divulgation sont en constante augmentation. La suppression ou l'altération de

données peuvent avoir des répercussions très graves, et sont parfois le fait d'un employé licencié ou malveillant.

6.2.4. Processus de gestion des risques

La gestion des risques passe par plusieurs étapes, liées les unes aux autres par un processus itératif et dynamique. Cette méthode est loin d'être rigide ou linéaire : elle varie en fonction du contexte interne ou externe, des parties prenantes, mais aussi de l'évolution des menaces et des opportunités. Ce travail est conçu pour être applicable à toutes sortes d'entreprises, quel que soit leur secteur, et aide à bâtir une culture du risque structurée et efficace.

- **Établissement du contexte**

Le cadre et le contexte guident la gestion des risques : ils définissent les risques à étudier, leurs mesures, et les limites jugées acceptables. Il est important de s'y référer régulièrement pour que chaque décision prise aide l'organisation à atteindre ses objectifs. On examine pour établir le contexte :

- **Les facteurs externes** : politiques, économiques, sociaux, technologiques, juridiques, climatiques et environnementaux.
- **Les facteurs internes** : culture, gouvernance, structures, responsabilités et processus.

Une déclaration d'appétence au risque définit le type et le niveau de risque que l'organisation est prête à accepter. On définit également des critères d'analyse communs : les conséquences d'un risque, sa probabilité d'occurrence, le croisement des deux pour obtenir un niveau de risque global, et la capacité de l'organisation à absorber ces risques (INTERNATIONAL ISO31000, 2018, pp. 6-7).

- **Identification des risques**

Identifier les risques, c'est recenser, définir et lister les événements susceptibles d'avoir une influence positive ou négative sur la réalisation des objectifs de l'organisation. Cette étape demande des informations pertinentes, fiables et actualisées. Diverses méthodes peuvent être utilisées. Les éléments à prendre en compte sont :

- Les sources de risques, qu'elles soient évidentes ou cachées.
- Les causes, les événements, les menaces et les opportunités.
- Les faiblesses et les atouts de l'organisation.

- Les changements du contexte interne et externe.
- Les signes de l'émergence de nouveaux risques.
- La valeur des actifs et des ressources.
- Les impacts potentiels sur les objectifs.
- Les lacunes en matière de connaissances et la fiabilité des données disponibles.
- Les contraintes et facteurs temporels.
- Les hypothèses, biais cognitifs et perceptions des parties prenantes.

Il convient d'identifier les risques, même lorsqu'ils sont hors du contrôle direct de l'organisation. Un même risque peut avoir plusieurs effets, positifs ou négatifs, tangibles ou intangibles (INTERNATIONAL ISO31000, 2018, p. 8).

- **Analyse des risques**

  L'analyse des risques permet de comprendre la nature d'un risque et d'évaluer son niveau. Elle porte sur les causes, les conséquences, les probabilités, les scénarios possibles et l'efficacité des mesures de contrôle existantes. Le degré de détail dépend des données disponibles et des ressources mobilisables. Des méthodes qualitatives, quantitatives ou combinées peuvent être employées.

  Les éléments à prendre en compte sont : la probabilité d'occurrence, l'ampleur des conséquences, la complexité des interactions, les facteurs temporels et l'efficacité des contrôles existants. Les résultats de l'analyse peuvent être influencés par les biais cognitifs, les perceptions, la qualité des données et les limites des méthodes utilisées ; il convient de documenter ces éléments. Pour les risques très incertains et lourds de conséquences, il est conseillé de recourir à plusieurs techniques d'analyse combinées. Les résultats de cette phase orientent ensuite l'évaluation des risques et les décisions de traitement. (INTERNATIONAL ISO31000, 2018, pp. 8-9).

- **Évaluation des risques**

L'évaluation des risques consiste à comparer les résultats de l'analyse aux critères de risque établis au préalable, afin de décider si une action est nécessaire. Cette comparaison peut conduire à plusieurs décisions : ne pas agir, traiter le risque, affiner l'analyse, maintenir les mesures actuelles ou ajuster les objectifs.

Les décisions doivent intégrer le contexte global et les impacts, réels ou perçus, sur les parties prenantes. Les résultats doivent être consignés par écrit, transmis et approuvés aux niveaux adéquats de l'organisation. (INTERNATIONAL ISO31000, 2018, p. 9)

- **Traitement des risques**

Le traitement des risques consiste à choisir et à mettre en œuvre des actions visant à modifier, réduire ou maîtriser les risques identifiés. C'est un processus itératif incluant le choix des options de traitement, leur mise en œuvre, l'évaluation de leur efficacité, et l'appréciation du risque résiduel pour déterminer s'il est acceptable.

Le choix des options implique d'équilibrer les bénéfices attendus, les coûts engagés et les contraintes existantes. Plusieurs approches sont envisageables :

- **Éviter le risque** en abandonnant l'activité en cause.
- **Réduire la probabilité** de survenance du risque.
- **Limiter les conséquences** en cas de réalisation.
- **Transférer le risque** à un tiers, notamment par le biais d'une assurance.
- **Conserver le risque** s'il est jugé acceptable.
- **Tirer parti d'une opportunité** liée au risque.

Le traitement doit être en accord avec les objectifs de l'organisation, les ressources disponibles et les attentes des parties prenantes. Un suivi rigoureux est nécessaire, car les mesures prises peuvent s'avérer insuffisantes ou générer de nouveaux risques. Le risque résiduel doit faire l'objet d'une documentation, d'une surveillance et d'une réévaluation si nécessaire (INTERNATIONAL ISO31000, 2018, pp. 9-10).

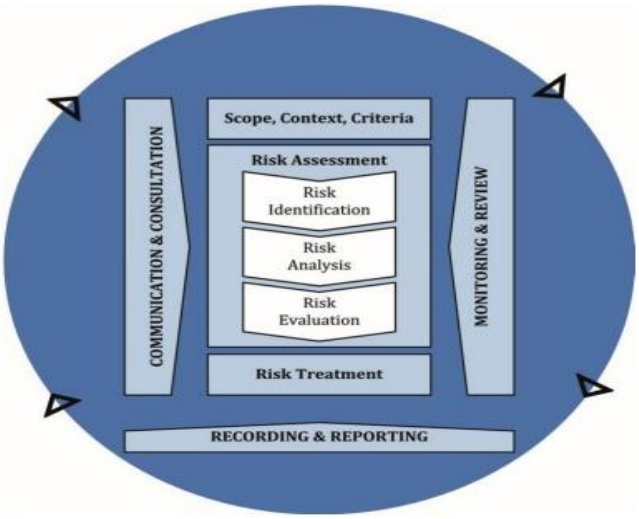
- **Surveillance et revue**

La surveillance et la revue ont pour objectif de veiller à la qualité et à l'efficacité du processus de gestion des risques et de l'améliorer en continu. À chaque étape du cycle (planification, collecte, analyse, enregistrement et restitution), un suivi continu et des contrôles réguliers sont prévus, avec des responsabilités clairement définies. Les données concernent la performance, les indicateurs de mesure et les comptes rendus**.**

Les résultats sont enregistrés et transmis pour éclairer les décisions, améliorer les pratiques et faciliter les échanges avec les parties prenantes. La transmission d'informations élément essentiel de la gouvernance, alimente le dialogue avec les parties prenantes et accompagne

la direction, en fonction des besoins, des coûts, de la fréquence, des méthodes et de la valeur des informations produites. (INTERNATIONAL ISO31000, 2018, pp. 10-11)

Figure 4: Processus de gestion des risques si.



Source : (INTERNATIONAL ISO31000, 2018)

7. Les Méthodes d'analyse des risques

7.1. Présentation de la méthode EBIOS : ((ANSSI), September 2024.)

La méthode EBIOS Risk Manager (EBIOS RM) a été développée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) avec le soutien du Club EBIOS ; il s'agit d'un référentiel méthodologique destiné à l'appréciation et au traitement des risques numériques. C'est une boîte à outils adaptable dont la mise en œuvre varie en fonction des objectifs propres à chaque projet, mais qui reste compatible avec les référentiels normatifs en vigueur dans les domaines de la gestion des risques et de la sécurité numérique. EBIOS Risk Manager permet ainsi d'évaluer les risques numériques, d'identifier les mesures de sécurité nécessaires à leur maîtrise mais également de valider un niveau de risque acceptable pour l'organisation. Elle s'inscrit également dans une logique d'amélioration continue sur le très long terme. Enfin, cette méthode permet de faire émerger les ressources et les arguments nécessaires à la communication interne et externe, ainsi qu'à la prise de décision stratégique au sein de l'organisation et avec ses partenaires. EBIOS Risk Manager a plusieurs finalités : la mise en place ou le renforcement d'un processus de gestion des risques numériques au sein d'une organisation ; l'évaluation et la prise en charge des risques attachés à un projet numérique, notamment dans le cadre d'une certification de sécurité ; définir le niveau de sécurité requis pour un produit ou un service, en fonction de ses cas d'usage prévus et des risques à contrer, dans une logique de certification ou d'agrément. La méthode s'applique

aux organisations publiques et privées, quelle que soit leur taille, leur secteur d'activité, et que leurs systèmes d'information soient en cours de conception ou déjà existants.

7.1.1. Une démarche interactive en 5 ateliers

Atelier01 : Cadrage et socle de sécurité

Ce premier atelier a pour but de définir l'objet de l'étude, les acteurs impliqués ainsi que le périmètre temporel. Vous y répertoriez les missions, les valeurs métier et les supports associés à l'objet analysé. Vous identifiez ensuite les événements redoutés susceptibles d'affecter ces valeurs métier, puis vous en évaluez la gravité potentielle. Enfin, vous examinez le niveau de conformité par rapport au socle de sécurité.

Atelier 2 : sources de risque

Identification des sources de risque Au cours de ce deuxième atelier, vous recensez et décrivez les sources de risque (SR) ainsi que leurs objectifs stratégiques, désignés sous le terme d'objectifs visés (OV). À l'issue de cet atelier, seuls les couples SR/OV jugés les plus significatifs sont conservés. Les résultats obtenus sont ensuite restitués sous la forme d'une cartographie des sources de risque.

Atelier 3 : Scénarios stratégiques

Lors de ce troisième atelier, vous commencez par acquérir une vision globale de l'écosystème et par établir une cartographie du niveau de dangerosité lié aux interactions avec les principales parties prenantes de l'objet étudié. Cette analyse vous permet ensuite d'élaborer des scénarios de haut niveau, appelés scénarios stratégiques. Ces derniers décrivent les chemins d'attaque qu'une source de risque pourrait emprunter pour atteindre son objectif. Ils sont construits à l'échelle de l'écosystème et prennent en compte les valeurs métier de l'objet étudié. La gravité de ces scénarios est ensuite évaluée. À l'issue de cet atelier, vous êtes déjà en mesure de proposer des mesures de sécurité applicables au niveau de l'écosystème.

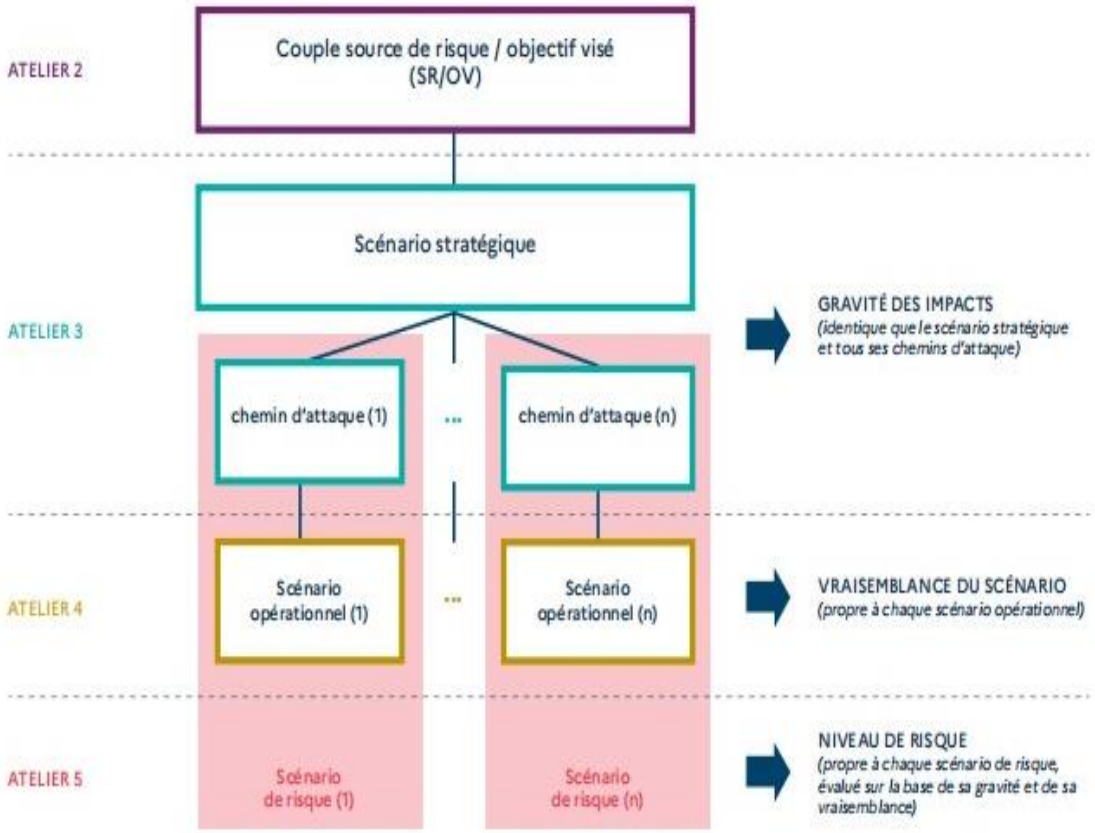
Atelier 4 : Scénarios opérationnels

Le quatrième atelier a pour objectif de construire des scénarios techniques détaillant les modes opératoires que les sources de risque pourraient mettre en œuvre pour concrétiser les scénarios stratégiques. Bien que sa démarche soit analogue à celle de l'atelier précédent, cet atelier se focalise spécifiquement sur les biens supports critiques. À l'issue de cet atelier, vous évaluez le niveau de vraisemblance de chacun des scénarios opérationnels ainsi élaborés.

Atelier 5 : Traitement du risque

Ce dernier atelier vise à rassembler l'ensemble des risques analysés et à définir une stratégie de traitement adaptée. Cette stratégie est ensuite déclinée en mesures de sécurité concrètes, intégrées dans un plan de traitement du risque. Au cours de cet atelier, vous réalisez également la synthèse des risques résiduels et vous établissez le dispositif de suivi des risques.

Figure 5 : Lien entre les différents ateliers.



Source : ((ANSSI), September 2024.)

7.2. Présentation la méthode MEHARI : (Clusif, 2022)

MÉHARI s'intéresse à la sécurité de l'information sous toutes ses formes : systèmes informatiques, données numériques, mais aussi supports analogiques et documents écrits. Il ne se contente pas d'identifier les situations à risque et d'évaluer leur niveau, mais cherche également à proposer des mesures concrètes pour réduire ces risques à un niveau acceptable. MÉHARI indique, pour chaque action recommandée, non seulement sa nature, mais aussi le niveau de qualité et d'efficacité attendu.

Enfin, tous les modules de MÉHARI sont fondés sur un principe de base : un risque ne doit jamais être négligé. En pratique, ce principe se décline en deux règles : toujours envisager le

cas le plus défavorable en termes de conséquences ; ne considérer que les effets réellement maîtrisés des mesures de sécurité.

7.2.1. La démarche de la méthode MÉHARI

→ **Étape 1 : Recherche et analyse des dysfonctionnements**

C'est l'étape la plus importante, car elle permet d'identifier les dysfonctionnements majeurs qui pourraient affecter les activités de l'organisation.

→ **Étape 2 : Classification des actifs**

On traduit les dysfonctionnements métier en risques techniques sur les actifs informatiques. Actifs primaires (données, services, processus) × critères de défaut → impact intrinsèque.

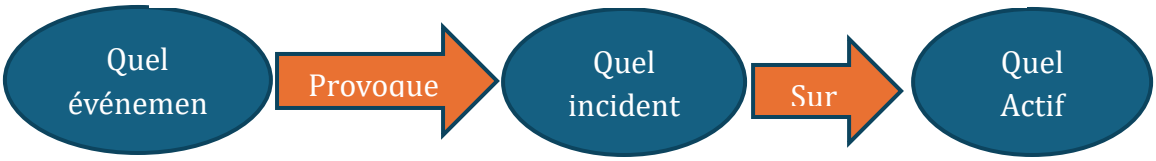
→ **Étape 3 : Diagnostic de l'état des services de sécurité**

On réalise un audit des services de sécurité (organisation, physique, informatique, etc.).

→ **Étape 4 : Paramétrage & Évaluation des risques**

On paramètre la méthode et on lance le calcul des risques. Pour chaque scénario (actif + événement déclencheur + dommage), on calcule la potentialité résiduelle (exposition naturelle réduite par la dissuasion et la prévention) et l'impact résiduel (impact intrinsèque réduit par le confinement et la palliation). La gravité finale est lue dans la grille d'acceptabilité (P × I → toléré / inadmissible / insupportable).

Figure 6: La logique de construction d'un scénario de risque.



-Type - dommage - actif primaire

-Circonstances - type de support

-Acteur

Source : (Clusif, 2022)

→ **Étape 5 : État des risques**

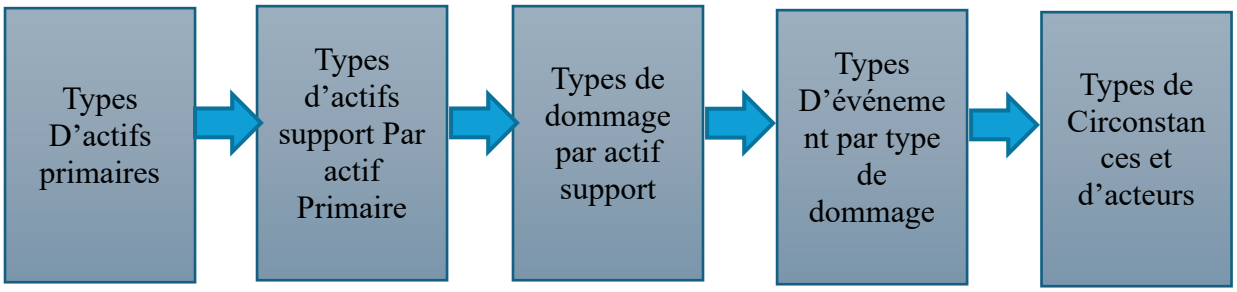
On visualise l'ensemble des risques sous trois angles : la grille globale I/P (nombre de scénarios par case), le panorama par type d'actif primaire et critère (D, I, C, E), et le

panorama par type d'événement déclencheur. Quatre options d'affichage sont disponibles : risques intrinsèques, actuels, résiduels ou futurs.

→ **Étape 6 : Traitement des risques**

On planifie les projets retenus et on officialise la décision pour les risques résiduels. Pour les risques qui restent après tous les projets, on décide de les accepter, de les éviter (en changeant l'organisation) ou de les transférer (par l'assurance).

Figure 7: La logique de traitement des risques MEHARI.



Source : (Clusif, 2022)

→ **Étape 7 : Indicateurs de suivi et tableau de bord**

On visualise l'efficacité du plan d'action dans le temps.

7.3. Présentation la méthode OCTAVE

La méthode OCTAVE est une collection structurelle d'outils destinés à aider dans l'évaluation et la planification stratégique pour assurer la sécurité des systèmes d'information, basés sur une analyse des risques. Le processus comprend trois phases interdépendantes.la phase initiale, dite organisationnelle, implique l'identification des informations actives critiques, ainsi que le processus actuel de leur protection. Sur cette phase, l'équipe aussi définit des besoins pour la sécurité de l'information et effectue une identification des risques. La deuxième phase, appelée technologique, fournit une évaluation de l'infrastructure technique. Cette phase implique une identification des informations techniques critiques, ainsi que la caractérisation des risques liés à ces actifs. Finalement, la troisième phase, dite d'évaluation des risques, utilise des informations recueillies lors des deux phases précédentes pour élaborer une stratégie de sécurité.

8. Les critères de choix de méthode de gestion des risques SI

Le choix d'une méthode de gestion des risques pour les systèmes d'information repose sur neuf critères stratégiques :

- L’origine géographique de la méthode : influence culturelle sur la perception du risque.
- La langue de la méthode : nécessité de maîtriser le vocabulaire employé.
- La qualité de la documentation garantit une appropriation correcte.
- La compatibilité avec une norme nationale ou internationale alignement avec des référentiels nationaux ou internationaux.
- Le coût de la mise en œuvre inclut coûts directs et indirects.
- Les moyens humains nécessaires et la durée de mobilisation disponibilité et compétences requises.
- L’adéquation à la taille de l’entreprise adéquation de la méthode à la structure.
- Le support assuré par l’auteur de la méthode pérennité du conseil et des mises à jour.
- La popularité de la méthode facilitée de recrutement de personnels qualifiés.

Tableau 1: Le tableau comparatif ci-dessous propose une vue synthétique des trois approches.

Critère	OCTAVE Allegro	MEHARI	EBIOS RM
Origine	CERT (États-Unis)	CLUSIF (France)	ANSSI (France)
Public cible	PME, équipes autonomes	Organisations structurées	Toutes tailles, haut niveau d'exigence
Approche	Axée sur les actifs informationnels	Axée sur les scénarios de dysfonctionnement	Axée sur les menaces et chaînes d'attaque
Complexité	Moyenne	Moyenne	Structurée (5 ateliers)

Sources : (pons, 2022)

9. Les enjeux de la gestion des risques en sécurité des systèmes d'information

a. Stratégiques et de gouvernance

- Continuité d'activité : prévenir une interruption de service causée par une menace (cyberguerre, dégradation, etc.).
- Prise de décisions informées : il faut que le top management prenne une décision en tenant compte du rapport coût/risques/bénéfices de l'entreprise.
- Gouvernance stratégique : être en phase avec la stratégie de l'entreprise et accompagner ses évolutions (techniques et technologiques).

b. Financières

- Piratage informatique : rançons, perte de chiffre d'affaires, coûts de remise en état de la situation, coûts contractuels.
- Frais indirects : hausse des primes d'assurances, perte de la capitalisation boursière, coûts de communication lors des situations de crise.
- Investissement : répartition entre la prévention, la détection, le contre-réactif.

c. Réglementaire et juridique

La mise en conformité de la sécurité des systèmes d'information se base sur une politique sécuritaire fondée principalement sur la Loi no 18-07 sur la protection des données à caractère personnel et les attributions qui sont données par cette loi à l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

d. Techniques et opérationnels

- Tendance à la complexité : hybride (cloud/on-Prem), travail à distance, IoT/OT.
- Menaces évoluant : rançongiciels, phishing sophistiqué, APT, attaque de déni de service.
- Gestion des vulnérabilités : priorisation des correctifs sans interruption de production.

e. Humains et organisationnels

- Facteur humain (premier risque) : erreurs, négligences, malveillance interne, ingénierie sociale.

- Culture de sécurité : passer de la contrainte à l'appropriation par tous les collaborateurs.
- Compétences rares : manque de professionnels de la cybersécurité et de la gestion des risques.

f. Sociétaux et de souveraineté

- Des infrastructures Critiques : énergie, eau, santé, transports, leur indisponibilité met la population en danger.
- Souveraineté des données : dépendance aux fournisseurs étrangers (cloud, logiciels) soumis aux lois extraterritoriales (CLOUD, etc.).
- Désinformation et ingérence : les SI peuvent servir de vecteurs à des campagnes d'influence ou à des vols de secrets d'État ou industriels.

De l’analyse des concepts de base de la littérature et des concepts de la sécurité des systèmes d’informations SSI et de gestion des risques découlent certains points de grande importance. Tout d'abord, il faut noter qu’une analyse de la littérature montre que bien que plusieurs études aient abordé la sécurité des systèmes d’informations et la gestion des risques en différents environnements organisationnels, ces études souffrent cependant de certaines lacunes dont notamment : l’absence d’étude de cas concernant des organismes financiers tels que la Direction Générale des Impôts (DGI), un niveau bas de conformité avec les normes ISO 27001 et un intérêt porté excessivement sur la sécurité physique au lieu de prendre en compte les risques liés aux systèmes fiscaux informatisés (paiement, déclaration et échanges de données). La sophistication progressive des systèmes d’informations fiscales SIF, exemplifiée ici par la DGI, rend compliqué l’application des méthodes sécuritaires conventionnelles et nécessite l’emploi de méthodologies adaptées. Ensuite, il faut évoquer le cadre conceptuel qui définit les éléments fondamentaux. Le système d’information est une structure intégrée qui sert à la collecte, à l’analyse, à la conservation et à la transmission des informations. La sécurité des systèmes d’informations fait référence à quatre aspects fondamentaux de protection dont la disponibilité, la fiabilité, la sécurité et la traçabilité pour protéger des biens informatiques face aux diverses menaces qui exploite leurs vulnérabilités. Le risque est le la combinaison entre la menace, la vulnérabilité et ses conséquences. L’ensemble des étapes du processus de gestion des risques (la compréhension du contexte, l’identification, l’analyse, l’évaluation, la gestion, la surveillance et l’évaluation) peut être considéré comme un processus répétitif et dynamique, nécessaire pour la gestion efficace des risques de sécurité. Un bon usage de ce processus ne sert pas seulement à minimiser les risques d’incidents, mais aussi d’améliorer la performance et la continuité du service public Pour conclure, ce chapitre souligne l'importance d'une approche systématique et structurée, tenant compte de la complexité du système d'information fiscal, afin de pouvoir obtenir une sécurisation réelle et une gestion proactive des risques dans la DGI.

CHAPITRE II

CADRE MÉTHODOLOGIQUE ET CONTEXTE ORGANISATIONNEL

La validité de toute étude repose sur la méthodologie qui est suivie pour la conduire. En particulier, cette méthodologie concerne les démarches utilisées pour obtenir les principales données de l'étude, c'est-à-dire les données et les procédures relatives à leur traitement. Dans ce chapitre, deux sections existent. La première section consiste à présenter L'organisme d'accueil, la deuxième section voire Le cadre Méthodologique de la recherche, par ailleurs, On a le choix du type d'étude, les instruments de mesure, la Collecte des données et la méthode de traitement des données.

Section 01 : Définition préliminaire de l'entité étudiée (Présentation de l'entreprise du stage)

Dans cette section, nous procédons à la présentation de Direction Générale des Impôts, en expliquant la structure Organisationnelle de cette dernière ainsi que son organigramme et les fonctions de la direction de gouvernance et sécurité de système d'information.

1. La présentation de la Direction Générale des Impôts DGI

La fiscalité est un élément important de l'économie nationale. Cette dernière a une importance stratégique dans la formation de fonds pour le développement économique, mobilisation des ressources internes de l'État et déduction de la dépendance aux autres sources financières. À cet effet, la Direction Générale des Impôts est importante étant donné qu'elle sert de moyen pour collecter les revenus fiscaux, améliorer la performance de la politique fiscale et créer un environnement favorable pour l'investissement

La Direction Générale des Impôts est une administration publique. Ses missions et ses organisations récentes sont définies par le décret exécutif n°21-252 du 25 Chaoual 1442 correspondant au 6 juin 2021, comme suit :

La Direction Générale des Impôts (DGI) est chargée de :

- De veiller à l'étude, à la proposition et à l'élaboration des textes législatifs et réglementaires ;
- D'assurer la mise en œuvre des mesures nécessaires pour l'établissement de l'assiette, la liquidation et le recouvrement des impôts, droits et taxes fiscales, ainsi que la perception des taxes parafiscales et autres produits ;
- De définir et de simplifier les procédures fiscales relatives à la gestion de l'assiette, du contrôle, du recouvrement et du contentieux de l'impôt ;
- D'élaborer les programmes stratégiques de modernisation et de s'assurer de leur mise en œuvre ;
- De développer et de déployer le système d'information et de mettre en place les interfaces et les outils de communication ;
- D'assurer la maîtrise d'ouvrages des référentiels en matière des technologies d'information et de communication ;

- De veiller à la préparation et à la négociation des conventions fiscales internationales et des accords internationaux comportant des dispositions fiscales ;
- De mettre en œuvre les mesures nécessaires de lutte contre la fraude et l'évasion fiscales
- De veiller à la prise en charge du contentieux administratif et judiciaire relatif aux impôts, droits et taxes de toute nature ;
- De mettre en place les instruments d'analyse et de contrôle de gestion de la performance des services fiscaux ;
- De veiller à l'amélioration des relations des services fiscaux avec les contribuables

2. L'organigramme de l'administration centrale

L'administration centrale est composée de **:**

- Trois (03) divisions :

- Division de la législation et de la réglementation fiscales et des affaires juridiques ;
- Division de la gestion du recouvrement et de la modernisation des processus métiers ;
- Division du contrôle et des enquêtes fiscales ;

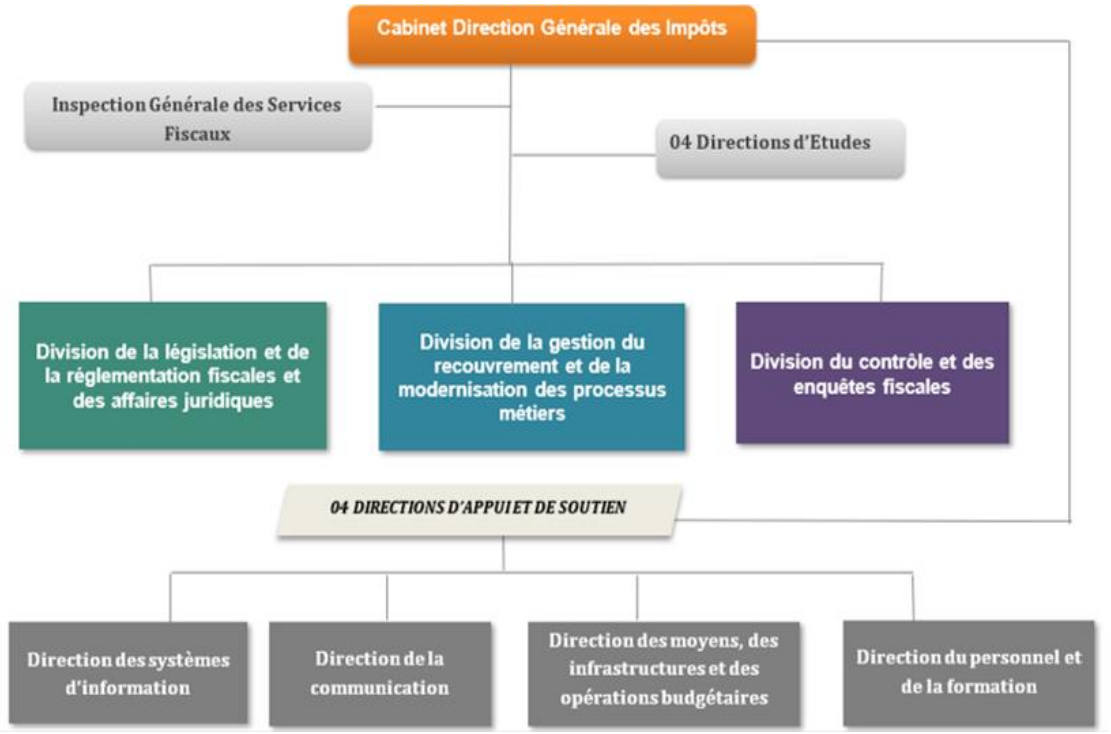
- Quatre (04) directions d'appui et de soutien :

- Direction des systèmes d'information ;
- Direction du personnel et de la formation ;
- Direction des moyens, des infrastructures et des opérations budgétaires ;
- Direction de la communication.

- Une Inspection Générale des Services Fiscaux *(IGSF),* régie par un texte particulier.

- Quatre (04) Directeurs d'Études, rattachés au cabinet du Directeur Général des Impôts

Figure 8: La Direction Générale des Impôts (DGI).



Source : (La Direction Générale des Impôts est une administration publique, s.d.)

3. Les Services de l'Administration Centrale

Ils sont 4 catégories

3.1. Les directions d'appui et de soutien : Sont

3.1.1. Direction des systèmes d'information : Est chargée de :

- Assurer la synergie du système d'information avec la stratégie globale et les exigences des métiers de la direction générale des impôts ;

- Intégrer au sein du système d'information les dernières évolutions technologiques enregistrées en la matière ;

- Assurer la gestion opérationnelle des systèmes applicatifs, des infrastructures, du réseau et de leur sécurité ainsi que d'apporter assistance et supports aux utilisateurs ;

- Etablir et de déployer la politique de sécurité visant à assurer l'intégrité des données, la sécurité des accès aux applications et aux équipements et la disponibilité des services fournis aux utilisateurs et aux contribuables.

Elle est composée de quatre (04) sous-directions :

A- La sous-direction des études et du développement : chargée notamment :

- D’assurer l’urbanisation des systèmes d’information à travers la mise en place du cadre architectural y relatif.
- De mener les études dans le cadre des évolutions de l'architecture fonctionnelle et technique projetées et d’évaluer l’opportunité de l’intégration des dernières évolutions technologiques.
- De procéder au développement des applications répondant aux besoins des services de la direction générale des impôts.
- De rédiger, en fonction des options stratégiques retenues, les termes de références relatifs aux spécifications techniques pour les besoins en acquisition et en réalisation de solutions logicielles.

B - La sous-direction de la gouvernance et de la sécurité des systèmes d’information fiscale : chargée notamment :

- De définir le plan stratégique des technologies de l’information de la direction générale des impôts et son alignement avec la stratégie globale tracée.
- De gérer le portefeuille des projets du système d’information et de définir les normes et méthodes qui lui sont applicables.
- De veiller à l’application des principes de gouvernance du système d’information, à travers l’établissement de tableaux de bord.
- D’assurer la sécurité et la fiabilité des systèmes d’information, à travers la définition et la mise en place de la politique de sécurité y relative.

C- La sous-direction de l’exploitation et du déploiement des solutions : chargée notamment :

- De définir et de maintenir les procédures opérationnelles d’exploitation des systèmes applicatifs.
- De superviser les activités de déploiement de nouvelles applications ou celles relatives à l’évolution des applications existantes.
- De veiller au fonctionnement des systèmes applicatifs par leur maintenance fonctionnelle et technique et d’assurer les supports aux utilisateurs et aux contribuables.

D- La sous-direction des équipements et du réseau et de la maintenance : chargée notamment :

- De déterminer les termes de références techniques afférentes aux acquisitions des équipements informatiques et aux contrats de maintenance, en prévision de l'évolution du système d'information en matière d'infrastructures systèmes et réseaux.
- D'assurer la gestion et la maintenance des équipements informatiques et de veiller à leur sécurité.
- D'assurer la continuité des services applicatifs et de support, à travers la mise en place d'un dispositif de secours et de reprise d'activités après interruption des services.

3.1.2. Direction du personnel et de la formation Est chargée :

- De la gestion des personnels, de leur suivi et de leur évaluation.
- De la conception des programmes de formation et de perfectionnement, du suivi de leur mise en œuvre et de leur évaluation.
- De définir et d'élaborer le dispositif de gestion des carrières et des compétences. Elle est composée de trois (03) sous-directions : La sous-direction du personnel et la sous-direction de la formation et du perfectionnement et la sous-direction de la valorisation des compétences et du suivi des carrières.

3.1.3. Direction des moyens des infrastructures et des opérations budgétaires : Est chargée de :

- Assurer l'exploitation, la maintenance et l'entretien des infrastructures et des équipements de l'administration fiscale.
- Etudier et d'élaborer les contrats d'équipement et d'approvisionnement des services.
- Elaborer les prévisions budgétaires et de veiller à l'exécution des budgets alloués.
- Evaluer les besoins des services, de gérer les moyens de fonctionnement et d'assurer l'entretien des infrastructures.
- Prendre en charge les contentieux relatifs aux marchés et conventions conclus. Elle est composée de trois (03) sous-directions : La sous-direction des moyens généraux et la sous-direction des infrastructures et des équipements et la sous-direction des opérations budgétaires.

3.1.4. Direction de la communication Est chargée **:**

- D'étudier et de prendre les mesures appropriées visant à améliorer les relations entre l'administration fiscale et les contribuables et de veiller à leur mise en œuvre effective par l'ensemble des services.

- D'élaborer et de diffuser les documents tendant à la vulgarisation de la législation et de la réglementation fiscales, en direction des citoyens et des personnels de la direction générale des impôts.
- D'élaborer et de diffuser les informations et avis, en direction des contribuables, relatifs à leurs droits et obligations en matière fiscale. Elle est composée de deux (02) sous-directions : la sous-direction de la communication, et la sous-direction des publications et des supports fiscaux.

Est chargée de :

- Définir et de simplifier les procédures relatives au contrôle et aux enquêtes fiscales.
- Concevoir les stratégies de lutte contre la fraude et l'évasion fiscales ainsi que de leur mise en œuvre.
- Assurer le suivi des activités de contrôle fiscal et d'en évaluer les résultats.
- Elle est composée de deux (02) directions : Direction du contrôle fiscal et Direction de la gestion de l'information et des enquêtes fiscales.

3.2. Division de la gestion du recouvrement et de la modernisation des processus métiers Est chargée :

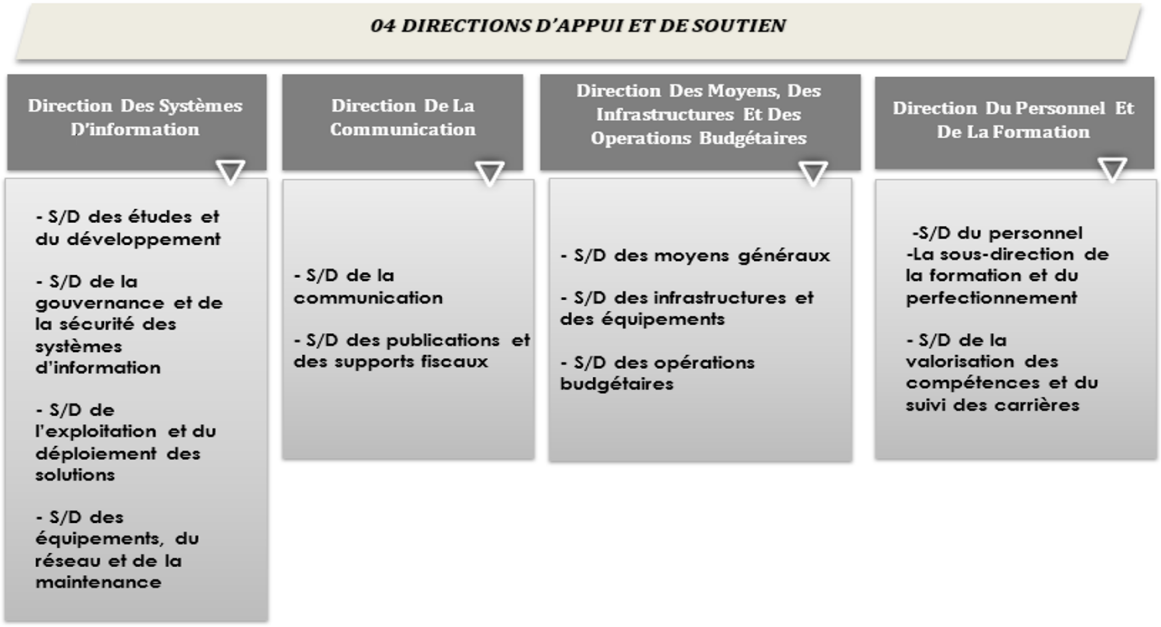
- De définir et de simplifier les procédures fiscales relatives à la gestion de l'assiette et du recouvrement.
- De veiller au suivi de l'activité des services, au titre de la fiscalité des personnes, des entreprises ainsi que de la fiscalité immobilière.
- D'assurer la prise en charge, sur le plan opérationnel, du volet relatif à la fiscalité des hydrocarbures et celle afférente à l'activité minière.
- D'élaborer la stratégie de modernisation des processus et procédures métiers de la direction générale des impôts, visant la facilitation de leur informatisation. Elle est composée de trois (03) directions : Direction de la gestion fiscale et Direction du recouvrement et des ressources fiscales locales et Direction de la modernisation des processus métiers et de pilotage.

3.3. Division de la législation et de la règlementation fiscales et des affaires juridiques Est chargée de :

- Mettre en œuvre la politique fiscale et d'élaborer les mesures législatives et réglementaires à caractère fiscal.

- Préparer et de coordonner les mesures de lois de finances et les textes d'application y afférents ; Participer à l'étude, à l'élaboration et aux négociations des projets de conventions et accords fiscaux internationaux et de veiller à leur mise en œuvre.
- Veiller à la bonne application de la législation et de la réglementation fiscales dans le traitement des affaires contentieuses. Elle est composée de trois (03) directions : Direction de la législation et de la réglementation fiscales et Direction des relations fiscales internationales et Direction du contentieux fiscal.

Figure 9: Direction du contentieux fiscal.



Source : (La Direction Générale des Impôts est une administration publique, s.d.)

1. Les Services Extérieurs

- Direction des grandes entreprises DGE.
- Inspection régionale des services fiscaux IRSF.
- Direction régionale des impôts DRI.
- Service régional des recherches et vérifications SRV.
- Centre régional de l'information et de la documentation CRID.
- Direction des impôts de wilaya DIW.
- Le centre des impôts CDI.
- Le centre de proximité des impôts CPI.
- Recette et inspection.

Section 2 : Cadre Méthodologie

Chaque étude menée dans le domaine des sciences de gestion s'inscrit dans différentes perspectives épistémologiques. Il est essentiel de choisir une approche pour guider notre travail et offrir une orientation claire aux lecteurs quant à notre démarche.

Dans le cadre de notre recherche, nous adoptons une posture épistémologique constructiviste. Cette approche cherche à générer de la connaissance en considérant que la réalité émerge des constructions mentales individuelles ou collectives, qui évoluent dans le temps. Cette perspective s'applique particulièrement bien à notre étude au sein de DGI où les dynamiques organisationnelles sont en constante évolution.

5. Approche méthodologique

La recherche s'inscrit dans une recherche qualitative en sciences de gestion. Il se concentre sur la recherche interventionnelle unique au sein des organisations publiques. L'approche qualitative est la plus appropriée car elle permet de comprendre et de répondre à la question initiale : Quelle est la meilleure façon d'assurer une meilleure gestion des risques de la sécurité de système d'information ?

Les méthodes qualitatives permettent également de considérer : La richesse des mots utilisés par les acteurs organisationnels. Comme (miles & huberman, 1991)l'ont souligné, les mots ont des caractéristiques « évocatrices », « spécifiques » et « significatives » plus convaincantes que les « chiffres ». Rechercher des faits socio-économiques à travers la littérature, des entretiens semi-directifs et des observations dans le « milieu naturel ». Ces deux raisons permirent de mieux cerner la complexité du phénomène à étudier. Quant au choix d'une recherche-intervention, comme stratégie de recherche, tel qu'elle est définie par Savall et Zardet (1995 : p104) « Cette recherche s'organise autour d'un processus d'interactivité cognitive entre les acteurs de l'entreprise et l'équipe de recherche », donc la RI consiste à aider, sur le terrain, à concevoir et à mettre en place des modèles, outils et procédures de gestion adéquats, à partir d'un projet de transformation plus ou moins complètement défini, avec comme objectif de produire à la fois des connaissances utiles pour l'action et des théories de différents niveaux de généralité en sciences de gestion selon (Albert DAVID,2000), semblé la plus appropriée pour aborder la question centrale de recherche.

5.1. Approche qualitative

Selon (Flick, 2018)la recherche qualitative consiste à immerger l'observateur dans le monde réel et à recourir à diverses techniques interprétatives permettant de rendre le monde intelligible. Ces techniques, telles que les notes d'observation, les entretiens, les photographies, les enregistrements et les mémos personnels, transforment le monde en un ensemble de représentations Cette méthodologie de recherche est naturaliste et interprétative, car elle étudie les phénomènes

Dans leur contexte naturel, en essayant de les comprendre au travers des significations que leur accordent les individus. Saisir un phénomène sociétal ou humain nécessite d'adopter une perspective approfondie et détaillée, en utilisant différentes méthodologies et en offrant une vision d'ensemble du cadre dans son environnement naturel. C'est là l'essence même d'une stratégie de Recherche qualitative.

Cette approche permet aux chercheurs de développer une compréhension approfondie d'un sujet Émergent et encore peu exploré. Elle met également l'accent sur la nécessité d'appréhender la problématique d'étude d'un point de vue humaniste ou philosophique (I.Baikady & A.Khan., 2022).

5.1.1. **Les Raisons de choisir l'analyse qualitative**

1. Le sujet traité Ce sujet est un sujet de caractère complexe et multidimensionnel, surtout si le thème concernant la gestion de risques de la sécurité des systèmes d'information est examiné. En effet, le sujet est multidimensionnel puisqu'il implique non seulement des questions techniques, mais également des questions organisationnelles et humaines, voire stratégiques. Il faut souligner que son étude nécessite une connaissance approfondie de l'environnement global de la DGI et des relations entre les parties prenantes. En outre, une analyse de la situation réelle sur place est requise, ce qui ne peut être fait sans une analyse qualitative.
2. La nature des phénomènes ou comportements étudiés Parmi certains phénomènes et comportements étudiés lors de cette sorte de recherche, on trouve ceux qui sont immatériels, et leur mesure n'est pas une chose facile. Par exemple, on peut citer le comportement des utilisateurs d'Internet, la culture de sécurité de l'information, ou encore la prise de décisions dans une organisation. Les phénomènes mentionnés sont complexes, ambigus, et leur analyse nécessite certaines conditions, et pas uniquement la mesure.

3. L'approche qualitative semble vraiment la plus adaptée pour ce genre de sujet. Elle permet d'aller plus en profondeur dans la compréhension des phénomènes en analysant les discours, les pratiques et les expériences des personnes concernées. Cette méthode aide à recueillir des données riches, détaillées et bien contextualisées, ce qui facilite l'interprétation des relations entre différentes variables. En plus, cette approche est flexible, ce qui permet aux chercheurs d'ajuster leurs outils au fur et à mesure que la situation évolue.
4. Les limites du questionnaire dans l'obtention de résultats fiables Concernant les questionnaires, même s'ils sont souvent utilisés dans la recherche scientifique, ils ont leurs limites, surtout quand on traite des sujets complexes. Parfois, ils ne suffisent pas à capturer la profondeur des informations qu'on recherche, surtout si les questions sont trop générales ou mal formulées. Voilà un petit aperçu des défis.
5. Le manque de fiabilité des réponses des répondants (notamment dans les questions fermées) Le problème de la fiabilité des réponses est vraiment important quand on utilise des questionnaires, surtout avec des questions fermées. Les gens doivent souvent choisir parmi des options qui ne correspondent pas toujours à ce qu'ils pensent ou à leur situation. En plus, certaines personnes peuvent se sentir obligées de donner des réponses qui semblent socialement acceptables, plutôt que ce qu'elles ressentent réellement. Cela peut créer des biais qui risquent de fausser les résultats globaux.

6. Méthode de collecte de données

6.1. **Observations**

Dans notre vie quotidienne, nous sommes souvent témoins de divers aspects du monde qui nous entoure. Ces observations, qu'elles concernent des objets, des événements ou des phénomènes, exercent une influence significative sur nos attitudes, nos comportements et nos croyances. Dans le but d'enrichir nos connaissances et nos méthodologies, ainsi que de mieux appréhender le déroulement des différentes opérations, nous avons choisi d'adopter l'observation comme méthode de collecte de données dans notre recherche (I.Baikady & A.Khan., 2022).

D'après leur définition, l'observation consiste à examiner délibérément des événements, des comportements ou des objets dans un but spécifique. Les explications fournies dans les dictionnaires correspondent à cette notion. Par exemple, le dictionnaire Macmillan décrit "l'observation" comme "l'action de regarder attentivement quelqu'un ou quelque chose dans le but d'apprendre quelque chose". De manière similaire, le dictionnaire Oxford définit

"l'observation » comme "le processus consistant à observer ou surveiller attentivement quelque chose ou quelqu'un".

6.2. **Analyse documentaire**

L'analyse de documents est une méthode rigoureuse employée pour examiner et évaluer une gamme étendue de documents, qu'ils soient imprimés ou numériques, incluant les contenus en ligne. Cette approche qualitative de recherche implique l'analyse approfondie et l'interprétation des données afin d'en extraire des significations, de saisir des concepts et de construire des connaissances empiriques. Diverses ressources telles que les registres de présence, les programmes d'événements, les manuels, les livres, les brochures, les journaux intimes, les journaux, les communiqués de presse, les données d'enquête, les documents publics, et même les albums photos et les coupures de presse peuvent être utilisées pour mener une analyse exhaustive (G.A.Bowen, 2009, pp. 27 - 40).

Durant notre recherche, nous avons consulté une variété de sources, incluant des bibliothèques et des plateformes en ligne telles que ResearchGate, Google Scholar, Z-Library, Scribd et SNDL. Ces ressources nous ont permis de découvrir de nombreux ouvrages, articles, et autres documents qui ont enrichi notre étude. Les bibliothèques de l'ENSM a également été source importante, offrant un accès à des travaux académiques et à des publications rédigées par des étudiants et des enseignants. Par ailleurs, l'accès aux archives et à la base de données de la DGI et le site officiel nous a été bénéfique, en ouvrant de nouvelles perspectives pour notre recherche et en consolidant nos conclusions. En plus des documents fournis par le bureau de la sécurité de système d'information relevant de la direction du système d'information de la Direction générale des impôts.

6.3. **L'entretien**

L'entretien est une méthode de collecte de données primaires couramment utilisée en recherche qualitative. Il implique une interaction entre le chercheur et un ou plusieurs participants, au cours de laquelle le chercheur pose des questions pour obtenir des informations sur un sujet spécifique. Les entretiens peuvent être réalisés de manière individuelle ou en groupe, et ils peuvent être structurés ou non structurés. Les entretiens individuels permettent au chercheur d'obtenir des informations détaillées et personnelles sur les participants, tandis que les entretiens de groupe favorisent les interactions et les échanges entre les participants. Ils sont souvent utilisés pour recueillir des données sur les expériences, les opinions et les perceptions des participants (A.Raymond, 1999). Nous avons choisi de recourir à des entretiens semi-

structurée dans le cadre de notre étude. Cette approche nous permettra d'explorer en profondeur les perspectives et les expériences des membres du bureau de la sous-direction de la gouvernance et de la sécurité des systèmes d'information fiscale, ce qui nous aidera à obtenir des données plus riches et nuancées. De plus, la nature semi-structurée de l'entretient nous offre la flexibilité nécessaire pour ajuster nos questions en fonction des nouvelles découvertes tout au long du processus d'étude, ce qui facilite l'adaptation aux nouvelles informations et aux résultats inattendus.

6.3.1. **L'entretien semi-directif**

Les entretiens semi-structurés sont une méthode d'entrevue où un ensemble de questions de base est utilisé pour orienter la discussion, tout en offrant à l'intervieweur ou à l'interviewé la possibilité d'approfondir un concept ou une réponse spécifique. Ce type d'entrevue est souvent privilégié dans le domaine de la santé car il guide les participants sur les sujets à aborder, ce qui est généralement apprécié. Par rapport aux entretiens structurés, les entretiens semi-structurés offrent une plus grande flexibilité, permettant ainsi d'identifier ou de développer des données que les participants jugent pertinentes mais que l'équipe de recherche n'avait peut-être pas envisagées initialement (Gill, tewart, Treasure, & Chadwick, 2008).

6.3.2. **Le guide d'entretien**

Le guide d'entretien joue un rôle essentiel en assurant la cohérence des entretiens en servant de référence et d'aide-mémoire. Son but principal est de maintenir une uniformité tout au long des entretiens afin de faciliter une comparaison efficace entre eux. Il vise notamment à garantir que les sujets cruciaux sont abordés de manière cohérente dans tous les entretiens, ce qui permet ensuite une évaluation et une comparaison approfondies des données collectées.

L'intervieweur a la liberté d'explorer de nouveaux sujets qui peuvent émerger au cours de l'entretien, sans être limité par le guide d'entretien. Ce dernier est utilisé lors d'entretiens semi structurés et comprend quelques directives initiales ainsi qu'une liste des sujets importants à aborder avec les participants. Bien que l'ordre de discussion de ces sujets puisse offrir un cadre pour l'entretien, le guide n'a pas pour but de le contraindre. Au contraire, l'entretien devrait évoluer de manière naturelle, en suivant le flux et la direction dictés par les réponses de l'interviewé (Wittorski & Daverne-Bailly, 2022).

Dans la sélection de nos interlocuteurs, nous avons opté pour une approche d'échantillonnage raisonné, inspirée de la méthode préconisée par (Thiétart, 2014). Ce processus, également désigné comme "sampling par jugement", repose sur le discernement du chercheur dans le

choix des participants. Il est considéré aussi efficace que les méthodes probabilistes, notamment pour des échantillons de petite taille.

Dans le cadre de cette étude, trois entretiens ont été conduits avec le chef du bureau de la sous-direction de la gouvernance et de la sécurité des systèmes d'information fiscale et son équipe Nos interviewés pour les entretiens semi-directifs sont donc choisis en fonction de leur expérience et de leurs contributions aux missions de gestion des risques. Les entretiens ont été menés en personne ainsi que par téléphone avec l'accord préalable des interviewés, et des enregistrements ont été effectués dans le respect des consentements obtenus

Ainsi, nous avons sélectionné un groupe de fonctionnaires de la Direction générale des systèmes d'information pour mener des entretiens avec eux, en les considérants comme un échantillon représentatif. À travers ces entretiens, nous avons abordé les aspects liés à la gestion des risques et à la sécurité des systèmes d'information au sein de la Direction générale des impôts. Les participants ont été choisis en fonction de leurs rôles et de leurs postes au sein de la direction. Leurs noms, fonctions et les périodes des entretiens sont présentés dans le tableau suivant :

Tableau 2: Liste des interviewés.

Entretien	Postes	Date et lieu	Durées des entretiens
Entretien 01	Membre du bureau de la sous-direction de la gouvernance et de la sécurité des systèmes d'information fiscale	08-04-2026 DGSSI	25min
Entretien 02	Membre du bureau de la sous-direction de la gouvernance et de la sécurité des systèmes d'information fiscale	08-04-2026 DGSSI	25min
Entretien 03	Le chef du bureau de la sous-direction de la gouvernance et de la sécurité des systèmes d'information fiscale	08-04-2026 DGSSI	30min

Source : établis par nous-mêmes

6.3.3. **Analyse des données qualitatives**

L’analyse des données qualitatives est un processus méthodique visant à évaluer des données non numériques telles que les textes, les images et les vidéos, dans le but de parvenir à une compréhension approfondie des expériences humaines et des comportements des individus. Ce type d’analyse est largement utilisé dans divers domaines tels que les sciences sociales, la psychologie et les études de marché.

Il repose sur plusieurs techniques, notamment l’analyse de contenu, la théorie ancrée (Grounded Theory), l’analyse narrative, l’analyse du discours et l’ethnographie, avec un accent particulier sur l’analyse thématique en tant qu’outil flexible permettant d’identifier des schémas et de comprendre les significations sous-jacentes (Creswell & W, 2018). Ce processus comprend plusieurs étapes, à commencer par la collecte des données, suivie de leur codification et de leur organisation en thèmes. Il s’appuie également sur des logiciels tels que NVivo, qui développé par QSR International, est l'un des logiciels les plus populaires pour l'analyse des données de recherche qualitative. Conçu spécifiquement à cet effet, il permet aux chercheurs de stocker, gérer, organiser, analyser et visualiser les données de manière intuitive, facilitant ainsi la rédaction et la discussion des résultats à la phase finale de la recherche.

En outre, la collecte des données nécessite la vérification de leur fiabilité, la suppression des informations non pertinentes, leur réorganisation afin d’en améliorer la gestion, ainsi que la mise en contexte nécessaire pour renforcer la précision de l’analyse et la clarté de l’interprétation (Solomon & DR Cox , 2014).

En conclusion de ce chapitre, il apparaît que l'adoption d'une méthodologie de recherche scientifique rigoureuse, associée à un choix approprié des sources de données, constitue une base essentielle pour garantir la qualité et la crédibilité de l'étude. Le recours à une méthodologie qualitative nous a permis d'acquérir une compréhension approfondie des pratiques de gestion des risques liées à la sécurité des systèmes d'information, à travers l'exploration de la réalité organisationnelle de la Direction Générale des Impôts dans ses dimensions environnementales, structurelles et organisationnelles. Par ailleurs, l'analyse des perceptions et des expériences des acteurs concernés, en s'appuyant sur des outils tels que l'entretien semi-directif et l'observation participante, a permis de mettre en évidence la diversité des points de vue et de mieux saisir la complexité caractérisant ce domaine. Grâce à cette interaction directe avec le terrain d'étude, nous avons pu recueillir des données riches constituant une base solide pour mener une analyse approfondie, prenant en considération les différents contextes entourant le sujet.

CHAPITRE III

RESULTATS ET DISCUSSIONS

Le système d'information de la Direction générale des impôts constitue l'un des systèmes les plus sensibles et complexes dans l'environnement numérique de l'administration algérienne. Il repose sur des bases de données volumineuses qui touchent directement à la vie financière des citoyens et des entreprises. D'où la nécessité impérative de comprendre ce système de l'intérieur, non seulement en termes de fonctionnalités, mais également en identifiant ses faiblesses et les sources de risques qui l'entourent.

Par ailleurs, la question de la sécurité des systèmes d'information dans un contexte de gestion fiscale ne se limite pas aux aspects techniques. Elle englobe également la confiance des citoyens envers les institutions de l'État, ainsi que la continuité d'un service public qui ne peut tolérer ni interruption ni fuite d'informations. Ainsi, toute défaillance ou intrusion ne produit pas uniquement des effets techniques, mais peut également porter atteinte à la légitimité même de l'institution.

Dans cette perspective, ce chapitre vise à proposer une analyse approfondie et multidimensionnelle de la problématique de la gestion des risques au sein de la Direction générale des impôts. Il s'appuie sur la présentation des expériences de trois pays en matière de gestion des risques liés à la sécurité des systèmes d'information dans le secteur fiscal, afin d'en tirer des enseignements et d'identifier les points forts et les limites, tout en s'inspirant des modèles internationaux sans tomber dans une imitation systématique. Enfin, ce travail inclut une description des systèmes d'information adoptés au sein de la direction, permettant de mieux comprendre l'environnement dans lequel les risques émergent, ainsi que l'application de la méthodologie EBIOS Risk Manager au contexte de la Direction générale des impôts.

Section 01 : Résultats

1. Présentation des résultats

Dans cette section, nous procéderons à une analyse détaillée des résultats des observations et entretiens réalisés auprès des employés, en explorant divers aspects de leur perception du processus de gestion des risques et sécurité des systèmes d'informations.

1.1. Résultats des entretiens

Les entretiens menés auprès les membres de bureau de sécurité de système d'information de la direction systèmes d'informations dans DGI ont permis de dégager une vision globale de la stratégie actuelle de gestion des risques.

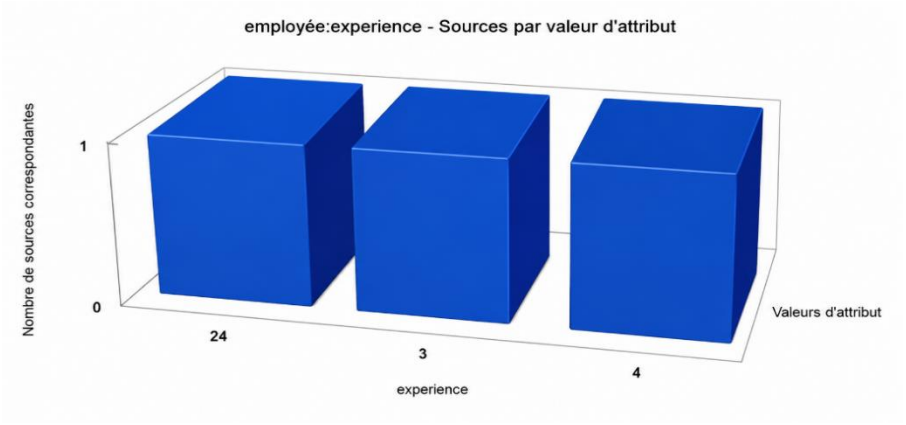
Pour apprécier convenablement le travail d'interview, cette section est scindée en deux parties fondamentales. La première partie s'attèle à une vue d'ensemble des entretiens, avec la caractérisation de l'échantillon et un coup d'œil sur l'analyse lexicale et textuelle, alors que la seconde partie s'attaque à la recherche thématique des différents thèmes traités par le guide d'entretien.

1.2. Analyse descriptive

L'analyse descriptive est une méthode d'exploration des données qui vise à résumer, organiser et présenter de manière claire les principales caractéristiques d'un corpus ou d'un ensemble d'informations recueillies. Elle repose généralement sur des outils statistiques simples (moyennes, fréquences, écarts-types, etc.) ou sur des représentations graphiques (tableaux, graphiques, nuages de mots) afin de dégager les tendances générales, les régularités et les particularités du matériau étudié, sans chercher à établir de relation de cause à effet.

La variable « expérience professionnelle » a été retenue comme indicateur principal pour évaluer la diversité et la richesse des profils des personnes interrogées. Comme l'illustre le graphique ci-dessus, l'échantillon comprend trois répondants ayant des niveaux d'expérience différents : l'un dispose de 24 années d'expérience professionnelle, le second de 3 années, tandis que le troisième compte 4 années d'ancienneté.

Figure10: graphique d'ancienneté Source réaliser avec NVIVO.



Source : réalisé avec NVIVO

Ces résultats reflètent une diversité des niveaux d'expérience au sein de l'échantillon, combinant un employé doté d'une longue et solide expérience avec des employés relativement récents dans le domaine. La présence d'un répondant ayant 24 ans d'expérience traduit un capital important de connaissances organisationnelles et de mémoire institutionnelle, ainsi qu'une compréhension approfondie de l'évolution des systèmes d'information au sein de la Direction Générale des Impôts, et des différents risques de sécurité auxquels ils peuvent être confrontés au fil du temps, tels que les risques de violation de données, les pannes techniques ou encore les menaces liées aux accès non autorisés.

En revanche, les deux répondants disposant de 3 et 4 années d'expérience apportent une vision plus récente, et sont potentiellement plus familiarisés avec les technologies modernes et les nouvelles pratiques en gestion des risques, telles que l'utilisation d'outils de surveillance numérique, des systèmes de détection des menaces et des mécanismes de protection avancés.

Cette complémentarité entre expérience approfondie et vision contemporaine constitue un élément positif pour l'étude, car elle permet de combiner une perspective stratégique fondée sur une longue expérience de terrain avec une approche moderne des défis sécuritaires et des opportunités d'amélioration du système de gestion des risques liés à la sécurité des systèmes d'information au sein de la Direction Générale des Impôts.

Ainsi, malgré la taille réduite de l'échantillon, la diversité des niveaux d'expérience professionnelle contribue à fournir une analyse plus approfondie et réaliste, et aide à identifier les forces et les faiblesses du système actuel, tout en proposant des solutions

concrètes pour renforcer la sécurité des systèmes d'information et réduire les risques potentiels.

1.3. Analyse textuelle des données

L'analyse textuelle consiste à examiner les discours recueillis à travers les entretiens dans le but d'identifier les structures linguistiques, les régularités lexicales et les usages terminologiques propres aux participants. Elle permet de mettre en évidence les termes les plus fréquemment employés, les cooccurrences significatives, ainsi que les thématiques dominantes, en offrant ainsi une première lecture descriptive des contenus avant toute interprétation approfondie.

1.4. L'approche lexicale

L'approche lexicale permet d'explorer les fréquences d'occurrence des mots dans le corpus des entretiens afin de mettre en évidence les termes dominants. Elle constitue une première étape d'analyse, offrant une lecture synthétique des discours recueillis et révélant les concepts clés, les préoccupations récurrentes ainsi que les champs thématiques les plus mobilisés par les répondants.

Le nuage de mots met en évidence les termes les plus récurrents dans les entretiens, notamment : gestion, sécurité, systèmes, information, risques, fiscales, données, développement, Jibaya'tic, Tabioucom, Qassimatouka, NIF et récupération.

Ces résultats confirment que les répondants accordent une importance particulière à la sécurisation des systèmes d'information, à la protection des données fiscales ainsi qu'à l'amélioration continue des processus de gestion des risques au sein de la DGI.

Figure 11:nuage de mots Source réalisé avec NVIVO

Source : réalisé avec NVIVO

1.5. L'approche linguistique

Est une méthode d'analyse qualitative qui s'intéresse à la manière dont le langage est utilisé dans un corpus de textes ou de discours, afin d'en dégager les intentions, les représentations et les structures argumentatives des locuteurs. Cette approche permet de mieux comprendre les mécanismes de communication, les stratégies discursives et les rapports de sens présents dans les entretiens.

Tableau3: des coefficients de corrélation (de Pearson) entre les entretiens.

Source A	Source B	Coefficient de corrélation de Pearson
interview 2	innterview 1	0,952753
interview 3	innterview 1	0,951111
interview 3	interview 2	0,946948

Source : réalisé avec NVIVO

Une analyse de la corrélation lexicale entre les trois entretiens a été réalisée afin de mesurer la similarité des réponses en termes de vocabulaire utilisé par les différents professionnels interrogés. Les résultats montrent un très fort niveau de cohérence lexicale entre les participants :

- L'entretien 02 et l'entretien 01 présentent une corrélation de 0,95, ce qui traduit une très forte similarité dans les idées abordées ainsi que dans le vocabulaire utilisé.
- L'entretien 03 est également très proche des deux premiers, avec une corrélation de 0,95 avec l'entretien 01 et de 0,95 avec l'entretien 02.

Cette forte proximité lexicale confirme la cohérence des discours recueillis et renforce la fiabilité des résultats thématiques. En effet, malgré la diversité des profils et des responsabilités des répondants, ceux-ci semblent partager une vision commune des enjeux liés à la gestion des risques associés à la sécurité des systèmes d'information au sein de la DGI, notamment en matière de protection des données, de continuité des services et d'amélioration des dispositifs de sécurité.

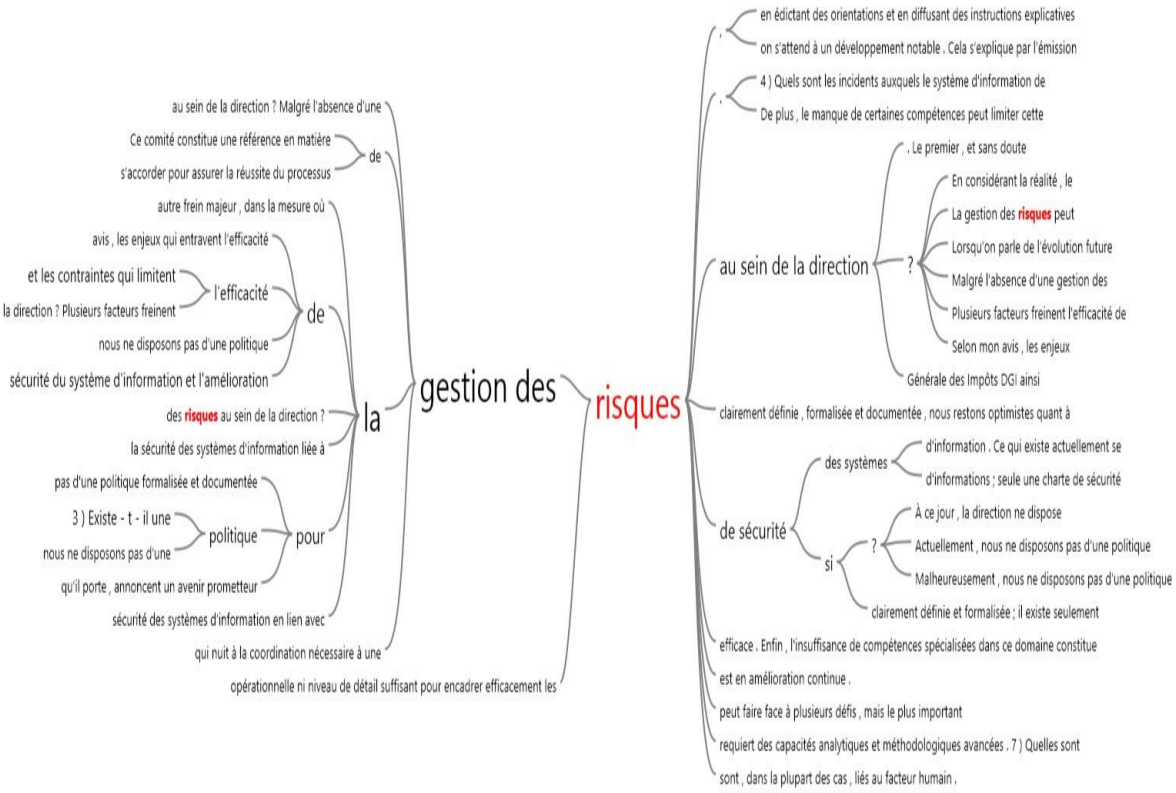
1.6. Cartographie cognitive

Afin d'approfondir l'analyse du contenu des entretiens, une cartographie cognitive permet de représenter visuellement les concepts évoqués par les participants et les liens entre eux. Cette approche met en lumière les idées dominantes et leur organisation autour des mots clés majeurs de cette recherche.

L'arbre de mots généré autour du terme « gestion des risques » liés à la sécurité des systèmes d'information au sein de la DGI révèle une association fréquente avec des notions de systèmes d'informations, de sécurité et de contraintes organisationnelles. Les données recueillies font ressortir des formulations telles que : « absence d'une politique formalisée », « manque de coordination », « insuffisance de compétences spécialisées » ou encore « contraintes qui limitent l'efficacité ».

Ces occurrences montrent que la gestion des risques est perçue comme un enjeu stratégique important, mais encore insuffisamment structuré. Toutefois, certaines expressions comme « amélioration continue » ou « avenir prometteur » traduisent une perception positive de l'évolution du dispositif.

Figure12: Requête corrélation sur le mot “risque “.



Source : réalisé avec NVIVO

L'arbre de mots généré autour du terme « fiscale » met en évidence son association avec des notions liées à la digitalisation des services et à la gestion des processus administratifs au sein de la DGI. Les données recueillies font ressortir des formulations telles que : «, Tabioucom », « NIF permet la création du numéro », « plateforme de déclaration Jibaya'tic » ou encore « Qassimatouka ».

Ces occurrences montrent que le domaine fiscal est fortement structuré autour des systèmes d'information, facilitant la traçabilité, la gestion des déclarations et les échanges avec l'administration. Elles soulignent également l'importance des outils numériques dans l'amélioration de l'efficacité, du suivi et de la transparence des opérations fiscales.

Figure13: Requête corrélation sur le mot “fiscale “.

Source : réalisé avec NVIVO

1.7. L'analyse thématique

Dans cette étude, l'analyse thématique a été menée à partir des entretiens réalisés auprès des acteurs de la Direction Générale des Impôts (DGI) voici l’annexe C. Les données ont été codées manuellement puis structurées sous forme de matrice d’analyse, permettant d'identifier les idées clés, les convergences et les divergences entre les participants. Cette approche met en évidence les principaux thèmes liés à la gestion des risques associés à la sécurité des systèmes d'information. L'interprétation s'appuie sur les extraits significatifs des discours afin de dégager une compréhension globale des pratiques actuelles et des axes d'amélioration.

➢ **Thème A :** Politique de gestion des risques SI

Les entretiens révèlent une absence quasi générale d'une politique formalisée et documentée de gestion des risques liés à la sécurité des systèmes d'information au sein de la DGI. Les participants soulignent que « nous ne disposons pas d'une politique clairement définie », et que les dispositifs existants se limitent essentiellement à « une charte de sécurité générale ». Cette situation traduit un manque de structuration stratégique, où la gestion des risques n'est pas encore encadrée par un cadre formel détaillé. Malgré cela, l'existence d'une politique générale de sécurité montre une première base, qui reste toutefois insuffisante pour couvrir efficacement l'ensemble des risques SI.

➢ **Thème B :** Organisation et cadre réglementaire

Les résultats mettent en évidence que la gestion des systèmes d'information s'inscrit dans un cadre réglementaire précis, notamment à travers des textes législatifs définissant les missions de la DSI. Les participants évoquent des responsabilités clairement établies, telles que la gestion des infrastructures, la sécurité des accès et l'intégration des nouvelles technologies. Cette structuration réglementaire constitue un point fort, car elle permet d'assurer une cohérence entre le système d'information et la stratégie globale de la DGI. Toutefois, cette organisation reste davantage orientée vers la gestion opérationnelle que vers une approche formalisée de gestion des risques.

➢ **Thème C** : Mesures de sécurité et protection des données

Les entretiens soulignent l'importance accordée à la sécurité des données fiscales, notamment à travers des mécanismes de sauvegarde et de restauration. Les participants mentionnent l'utilisation de solutions techniques avancées, ainsi que la mise en place d'un site miroir garantissant la disponibilité des données.

Des tests de restauration sont également réalisés pour évaluer la rapidité de récupération, avec des résultats jugés satisfaisants. Ces éléments montrent que la DGI dispose de mesures techniques solides pour assurer la continuité des activités, même si celles-ci ne s'inscrivent pas toujours dans une démarche globale de gestion des risques formalisée.

➢ **Thème D :** Défis et contraintes

L'analyse met en évidence plusieurs obstacles freinant l'efficacité de la gestion des risques. Le facteur humain apparaît comme le principal défi, notamment à travers le manque de

coordination, l'insuffisance de communication interne et le faible partage d'information entre les acteurs. Les participants soulignent également un manque de compétences spécialisées, ce qui limite la capacité à mettre en œuvre des approches avancées. Ces contraintes organisationnelles traduisent une difficulté à instaurer une gestion des risques efficace et collaborative.

➢ **Thème E :** Incidents et vulnérabilités

Les incidents identifiés sont classés en deux catégories principales : les incidents fonctionnels et les incidents de sécurité. Les premiers sont liés aux erreurs humaines, à la mauvaise compréhension des procédures ou au non-respect des bonnes pratiques.

Les incidents de sécurité, quant à eux, peuvent être d'origine interne ou externe, incluant des négligences (comme l'accès non sécurisé aux salles serveurs) ou des facteurs environnementaux. Cette classification met en évidence le rôle central du facteur humain dans la survenue des risques.

➢ **Thème F** : Perspectives d'évolution

Malgré les limites constatées, les participants expriment une vision globalement optimiste. Ils évoquent un « avenir prometteur » pour la gestion des risques, soutenu par des évolutions réglementaires récentes et des initiatives institutionnelles visant à renforcer la sécurité des systèmes d'information. La création de structures dédiées à la sécurité SI et l'implication des autorités supérieures sont perçues comme des leviers importants pour améliorer la maturité du dispositif. Cette dynamique montre une volonté d'évolution vers un cadre plus structuré et performant.

2. Analyse comparative des méthodes de gestion des risques mises œuvre dans divers contextes nationaux

Il existe trois méthodes reconnues dans le monde pour analyser et gérer les risques : EBIOS, MEHARI et OCTAVE.

1. **EBIOS** est un outil de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), une agence française. Il a été publié fin 2018. Cette méthode repose sur l'analyse des attaques possibles et des menaces. Elle comporte cinq étapes, allant du niveau général au niveau technique. EBIOS est la méthode officielle du gouvernement français. Elle est également utilisée par la Tunisie, la Suisse et le Luxembourg.
2. **MEHARI** est un outil d'audit qui examine les faiblesses en lien avec les objectifs de sécurité. Il s'appuie sur des référentiels préexistants et une base de données pour identifier les écarts techniques. Il est principalement destiné aux entreprises privées. Il a été créé par le CLUSIF (Club de la Sécurité des Systèmes d'Information Français).
3. **OCTAVE** a été conçue par le Software Engineering Institute (SEI) de l'Université Carnegie Mellon, aux États-Unis. Elle part des éléments importants de l'entreprise pour analyser ensuite les menaces internes et externes. Il existe trois déclinaisons : OCTAVE pour les grandes entreprises, OCTAVE-S pour les petites et moyennes entreprises, et OCTAVE Allegro pour les contextes actuels. Cette méthode est très utilisée aux États-Unis (gouvernement, armée, banques, santé), au Canada, au Royaume-Uni, en Australie, en Allemagne, aux Pays-Bas, ainsi que dans plusieurs pays d'Amérique latine (Brésil, Mexique, Argentine) et d'Asie (Singapour, Corée du Sud).

Ces trois méthodes offrent des points de vue différents (les menaces, les vulnérabilités et les actifs importants). Elles sont utilisées selon les régions et les secteurs d'activité.

2.1. Les avantages et inconvénients

a. Avantages de la méthode EBIOS

- Approche réaliste fondée sur des scénarios d'attaques stratégiques et opérationnelles.
- Correspondance aux besoins métiers (« valeurs professionnelles »).

- Adaptée aux systèmes critiques, au cloud et à l'IA (avec des nuances pour le cloud, la responsabilité partagée restant un défi).
- Conforme aux normes ISO 27005 et ISO 31000.
- Gratuite et indépendante (pas de liens avec des fournisseurs privés).
- Dernière importante mise à jour : EBIOS Risk Manager (2018), enrichie régulièrement par l'ANSSI.

b. **Limites de l'EBIOS**

- Complexité relative et temps d'application important.
- La subjectivité dans l'appréciation de la vraisemblance des attaques.

c. **Avantages de la méthode MEHARI**

- Richesse des bases de données (grilles d'audit « clés en mains »).
- Pratique pour pallier les lacunes techniques directes.
- Stable, éprouvée à long terme.

d. **Limites de la méthode MEHARI**

- Moins adaptable aux menaces rapides et émergentes.
- Documentation pesante et chronophage.

e. **Avantages d'OCTAVE**

- Une priorisation évidente vers les actifs critiques, ce qui oriente l'analyse vers ce qui mérite réellement d'être protégé.
- Il associe des acteurs de niveaux organisationnels variés (dirigeants, techniciens, utilisateurs) et renforce ainsi la sensibilisation.
- Avec les versions OCTAVE-S et OCTAVE Allegro, il n'est pas nécessaire de disposer d'une expertise technique très poussée.
- Conforme aux normes NIST et ISO 27005.

f. **Limites d'OCTAVE**

- L'accent mis très fortement sur les actifs peut masquer des menaces situationnelles ou des attaques non ciblées.
- La version originale est complexe et coûte très cher en temps dans les grandes organisations.
- Sa documentation est moins complète que celle d'EBIOS dans le cadre européen. Il n'y a pas de traduction officielle en arabe ou en français, ce qui pose problème dans les milieux maghrébins et francophones.

2.2. Arguments en faveur du choix d'EBIOS par la DGI algérienne

- **Adéquation institutionnelle** : EBIOS a été spécifiquement conçue pour les organismes publics et les organisations d'État. La DGI, en tant qu'administration fiscale de l'État algérien, constitue un domaine d'application naturel et optimal pour cette méthodologie. Elle s'inscrit par ailleurs dans le cadre de la politique nationale algérienne en matière de cybersécurité.
- **Protection des données fiscales sensibles :** La DGI traite des millions de données confidentielles relatives aux personnes physiques et morales, notamment leurs déclarations fiscales et leurs informations financières. EBIOS permet d'analyser les risques par scénarios d'attaques ciblées, couvrant les tentatives d'intrusion externes, les menaces internes, les fuites de données ainsi que les attaques par rançongiciels visant les infrastructures critiques.
- **Compatibilité avec les normes internationales** : EBIOS est conforme aux normes internationales ISO 27001, ISO 27005 et ISO 31000, ce qui facilite l'obtention de certifications internationales et le développement de partenariats techniques avec des institutions telles que le FMI, la Banque mondiale ou l'Union européenne.
- **Approche hiérarchique descendante :** La méthodologie part du niveau stratégique (direction générale) pour descendre jusqu'au niveau technique, garantissant ainsi l'implication de la haute direction et une mise en œuvre opérationnelle efficace au sein d'une institution hiérarchique telle que la DGI.
- **Gratuité, documentation et scalabilité :** elle est totalement gratuite, ce qui permet à l'État algérien de garder une souveraineté totale. Elle est entièrement documentée, avec des exemples de scénarios prêts à l'emploi. L'ANSSI publie régulièrement des
- **Mises à jour (dernier guide majeur :** EBIOS Risk Manager 2018, enrichi de puis pour le cloud et les nouvelles menaces).
- **Adoption internationale par les administrations fiscales** EBIOS est utilisée par plusieurs administrations fiscales dans le monde, notamment en Belgique, en Tunisie et au Canada (Québec), ce qui témoigne de sa robustesse et de son adaptabilité aux contextes institutionnels variés.

Donc EBIOS Risk Manager est la solution la plus reconnue, la plus justifiée et la mieux adaptée à la Direction générale des impôts algérienne : une méthode gouvernementale conforme aux normes internationales, centrée sur les scénarios d'attaque, gratuite, évolutive et alignée sur les meilleures pratiques des administrations fiscales francophones. La méthode OCTAVE, bien qu'elle soit reconnue dans les milieux anglo-saxons et académiques, n'est pas documentée officiellement en français et est éloignée du contexte institutionnel public francophone, ce qui en fait une méthode moins adaptée au contexte algérien qu'EBIOS.

3. Les outils de la gestion des risques

3.1. SimpleRisk

SimpleRisk est une plateforme de gouvernance, gestion des risques et conformité (GRC) open source qui se base sur la simplicité, l'accessibilité financière et l'efficacité. Elle permet aux organisations d'identifier, de classer, de surveiller et de suivre leurs risques tout au long du cycle de vie d'atténuation, tout en mesurant en continu la progression de leur programme de cybersécurité.

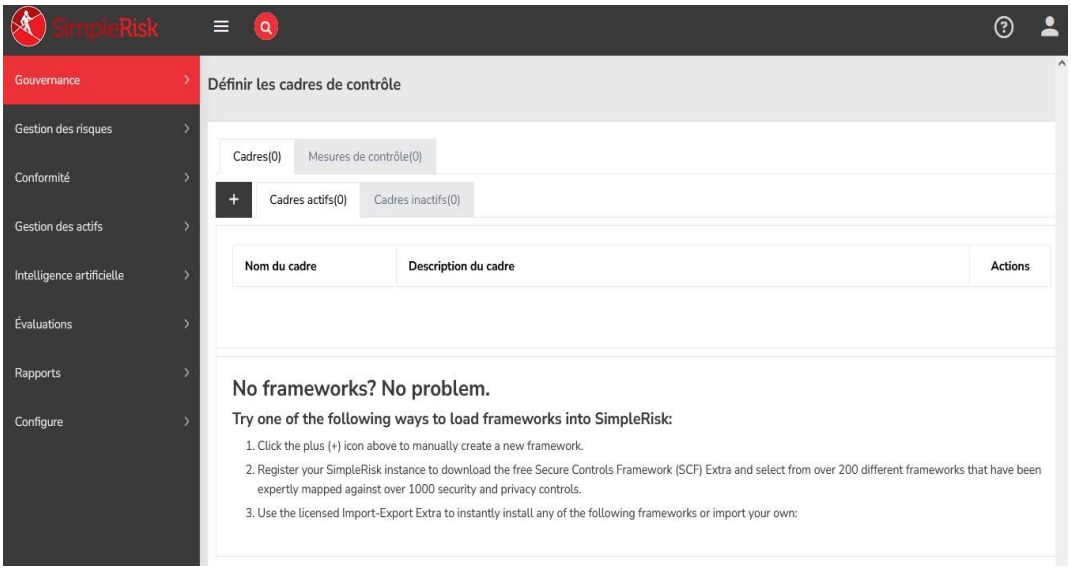
3.1.1. Fonctionnalités principales

- Gestion des risques fondée sur le classique Probabilité × Impact.
- Gestion d'incidents selon la méthodologie NIST 800-61 Évaluation des risques par questionnaires dynamique.
- Gestion des actifs et des règles Des tableaux de bord complets et des rapports d'audit. La plateforme gère plus de 250 référentiels de conformité (ISO 27001, NIST CSF, PCI DSS, RGPD…). Des extensions payantes viennent compléter l'offre : API RESTful, authentification AD/SAML, chiffrement AES-256.
- Séparation des risques au niveau des équipes Intégration avec Jira et les scanners de vulnérabilités (Tenable, Rapid7, Qualys).
- CSV import/export.

3.1.2. Côté public

SimpleRisk convient aux agences gouvernementales grâce à sa conformité aux normes NIST et sa capacité à séparer des niveaux de hiérarchie. Cependant, des extensions payantes sont nécessaires pour certaines fonctions critiques, telles que les notifications ou l'authentification unique. Par ailleurs, son modèle hébergé peut soulever des interrogations quant aux exigences de souveraineté des données.

Modèles de déploiement : Version gratuite Version hébergée Sa force réside dans : Simplicité d'utilisation, déploiement rapide, prix compétitif, support multilingue (35 langues) et une communauté d'utilisateurs très large – des startups aux gouvernements.



3.2. CISO Assistant

CISO Assistant est une plateforme open-source de gouvernance, gestion des risques et conformité (GRC) conçue pour aider les RSSI et les équipes sécurité à remplacer les tableurs et documents disparates par un système centralisé et structuré. Développé et maintenu par la société française intuitem, l'outil constitue une source unique de vérité pour gérer et corréler plus de 100 modèles de conformité (référentiels, normes, questionnaires sectoriels ou réglementations locales), tels qu'ISO 27001, NIST CSF, SOC 2, RGPD, PCI DSS, NIS2 (couverture évolutive)**,** DORA (en cours d'enrichissement)**,** CMMC ou encore l'Essential Eight, tout en permettant d'importer ses propres référentiels.

Parmi ses fonctionnalités clés figurent l'analyse d'écarts multi-référentiels, le mapping automatique des contrôles entre normes, l'évaluation des risques avec scores de risque inhérent et résiduel, la gestion des preuves avec workflows de validation, ainsi qu'un historique d'audit (niveau de détail adapté aux audits ISO 27001, mais pouvant nécessiter des compléments pour des exigences très strictes comme SOC 2 Type 2)**.** CISO Assistant intègre également un contrôle d'accès basé sur les rôles, une architecture orientée API pour l'intégration avec des outils existants comme Jira ou des SIEM, des tableaux de bord interactifs affichant l'état de conformité en temps réel et une cartographie des risques, ainsi qu'une génération automatique de rapports prêts pour l'audit.

Les organisations peuvent déployer l'outil sur site via Docker (avec maîtrise totale des données), utiliser une instance cloud hébergée par intuitem (données alors confiées à l'éditeur), ou opter pour une version entreprise payante ajoutant l'authentification unique, des droits avancés et un support prioritaire. L'édition communautaire, véritable cœur du produit, est publiée sous licence libre AGPLv3, garantissant l'absence d'enfermement propriétaire.

Pour les PME comme pour les grandes structures, CISO Assistant offre une alternative puissante aux solutions GRC commerciales coûteuses telles que One Trust ou RSA Archer, mais sans frais de licence (sous réserve des coûts d'infrastructure et d'administration en mode on-premise), ce qui en fait une solution particulièrement adaptée aux équipes soucieuses de leur budget qui souhaitent une gestion professionnelle de la conformité en gardant la maîtrise de leurs données (en déploiement local).

3.3. Archer

Archer est une plateforme intégrée de gestion des risques (IRM) conçue pour les agences publiques afin de répondre aux défis majeurs de l'assurance de l'information : conformité complexe (RGPD, NIS 2, LPM, référentiels ANSSI, ISO 27001), manque de visibilité contextuelle sur les risques, silos technologiques et organisationnels, rareté des ressources et contraintes budgétaires.

Elle centralise toutes les données de risque et de conformité dans un référentiel unique, s'intègre nativement aux scanners, capteurs et outils de sécurité existants, et propose trois modules clés :

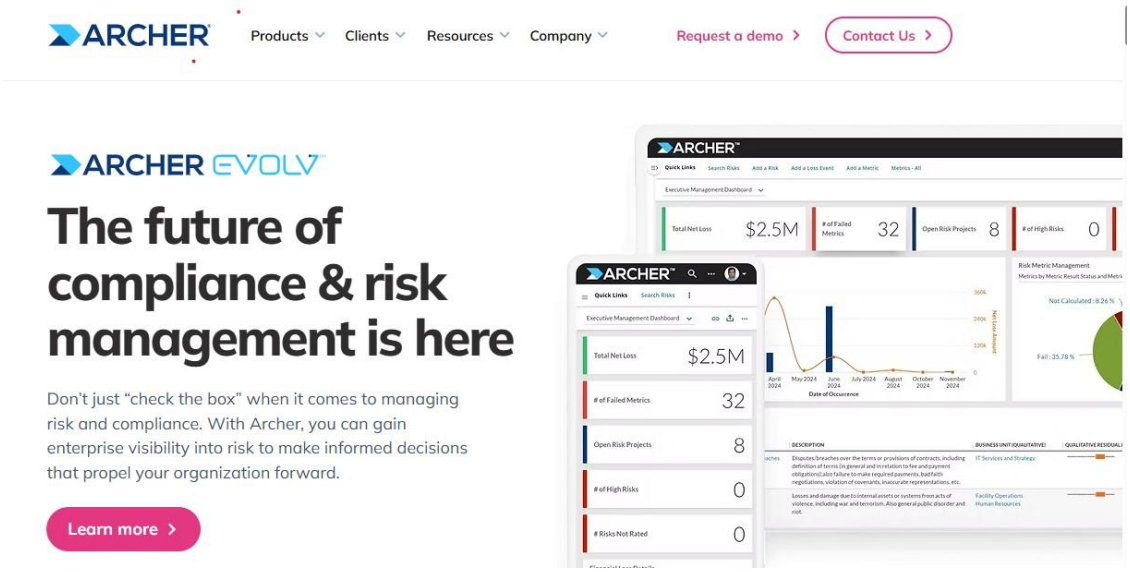
- Évaluation et Autorisation (gestion complète des cycles d'autorisation et habilitation continue).

- Surveillance continue (priorisation automatique des risques et évaluation continue des contrôles).
- Gestion du POA&M (centralisation des failles, suivi des plans d'action, jalons, coûts et approbations).

Grâce à cette approche, Archer supprime les silos, automatise la production des artefacts de conformité, permet une vue agrégée du risque à tous les niveaux avec le vrai contexte métier, et s'adapte rapidement aux évolutions réglementaires ou internes grâce à des workflows et tableaux de bord reconfigurables.

Résultats pour les agences publiques : réduction des coûts de main-d'œuvre et de formation, diminution des incidents de sécurité, amélioration de la culture commune du risque et meilleure valorisation des investissements existants. (Note : les économies portent sur les opérations, pas nécessairement sur le coût des licences.)

Contrairement à des solutions rigides et « codées en dur », Archer offre une véritable agilité. La plateforme s'appuie sur plus de 20 ans d'expérience et une base de clients solide, dont de nombreuses grandes organisations publiques et privées à l'international.



4. **Analyse académique des exigences de la Direction Générale Algérienne (DGI) :**

Cette analyse s'appuie sur les résultats du Tableau présenté en « **annexe D »** , intitulé « Comparatif complet des outils GRC

Sur la base de l'analyse des exigences de la DGI, la solution **CISO Assistant** se classe en première position comme la plus appropriée pour plusieurs raisons :

- Flexibilité totale de personnalisation selon le cadre national algérien, grâce à son code source ouvert (AGPL v3), permettant à l'équipe interne d'adapter le code à toutes les exigences nationales.
- Support complet de la méthodologie EBIOS RM (l'un des rares outils open source à le faire nativement, aux côtés d'autres solutions comme Monarc de l'ANSSI).
- Souveraineté totale sur les données via une installation locale, en cohérence avec la politique algérienne de souveraineté numérique et l'utilisation de centres de données nationaux (cloud gouvernemental).
- Architecture moderne en micro services permettant une expansion horizontale.
- Efficacité économique : la version communautaire est entièrement gratuite et adaptée au budget du secteur gouvernemental.

En **deuxième position** se trouve **Archer** comme une option circonstancielle très limitée :

- Standard mondial de référence, mais extrêmement coûteux (plus d'un million de dollars).
- Ne supporte pas nativement EBIOS RM (un paramétrage lourd et coûteux serait nécessaire, sans garantie de conformité complète).
- Ne s'adapte pas facilement au cadre algérien sans d'importants développements spécifiques.
- Recommandé uniquement dans le rare cas d'une collaboration étroite et imposée avec des agences américaines.

En **troisième** position se trouve **SimpleRisk** comme solution temporaire et non institutionnelle :

- Architecture PHP traditionnelle (moins flexible et moins adaptée aux déploiements à grande échelle qu'une architecture moderne).
- Version communautaire très limitée, dépourvue de fonctionnalités essentielles (gestion avancée des cadres, workflows).
- Ne supporte pas EBIOS RM nativement ; l'adaptation au cadre algérien est partielle et insuffisante pour un usage institutionnel.

- Peut convenir à un très petit bureau au sein de la DGI, mais pas à une utilisation à l'échelle de la direction générale.

L'ordre de priorité dans l'intérêt de la DGI est :

1. **CISO Assistant** : pour sa flexibilité, sa souveraineté, son support méthodologique (EBIOS RM) et son faible coût.
2. **Archer** : option circonstancielle, très coûteuse, uniquement envisageable en cas d'interopérabilité imposée avec des agences américaines.
3. **SimpleRisk** : solution temporaire inadaptée à un usage institutionnel durable.

5. Description du Système de la DGI (Direction Générale des Impôts)

La Direction Générale des Impôts (DGI) algérienne a mis en place un système fiscal numérique intégré, visant à moderniser et simplifier la gestion fiscale à travers plusieurs plateformes et services électroniques complémentaires.

5.1. Présentation de la plateforme "Tabi3okom"

Tabi3okom est une plateforme électronique relevant de l'administration fiscale algérienne, qui permet aux citoyens de payer les droits de timbre fiscal en ligne facilement et en toute sécurité, 24h/24 et 7j/7, sans avoir besoin de se déplacer. La plateforme se distingue par sa rapidité, sa sécurité et sa facilité d'utilisation, permettant le paiement électronique via une carte bancaire ou dorée, avec la possibilité d'imprimer le reçu dès que le paiement est effectué.

5.1.1. Étapes d'utilisation

Étape 1 : Remplir le formulaire d'informations personnelles.

Étape 2 : Vérifier les informations et choisir la catégorie et le type de document.

Étape 3 : Consulter et confirmer le type de document et le tarif du droit de timbre applicable.

Étape 4 : Saisir les informations de la carte de paiement bancaire ou dorée.

Etape 5 : Télécharger et imprimer le reçu de paiement.

La plateforme Tabi3okom incarne la transformation numérique de l'administration fiscale algérienne, et vise à simplifier les procédures fiscales tout en faisant gagner du temps et des efforts aux citoyens.

5.2. Présentation de la plateforme " Qassimatouka "

Qassimatouka est la plateforme d'acquisition de la vignette automobile en ligne. Ce service innovant vise à simplifier l'acquisition de votre vignette automobile de manière facile et rapide. Grâce à cette solution numérique, vous bénéficiez d'un gain de temps et d'une sécurité renforcée pour vos transactions. Vous pouvez effectuer votre paiement et télécharger la vignette instantanément, en seulement quelques clics.

5.2.1. Procédure d'obtention de la vignette en ligne

Etape 01 : Saisie du numéro d'identification du véhicule : veuillez introduire le numéro d'immatriculation de votre véhicule.

Etape 02 : Vérification des informations du véhicule et saisie des informations du propriétaire : veuillez vérifier l'exactitude des informations du véhicule, puis saisir les informations du propriétaire.

Etape 03 : Affichage du tarif du droit de la vignette applicable : veuillez confirmer le paiement du tarif applicable.

Etape 04 : Paiement du droit de la vignette automobile : veuillez introduire les informations de votre carte de paiement (CIB ou EDAHABIA).

Etape 05 : Téléchargement et impression : une fois le paiement effectué, vous pouvez procéder à l'impression de la vignette ainsi que de son reçu de paiement.

5.3. Présentation de la plateforme " Le NIF "

Le NIF (Numéro d'Identification Fiscale) est un identifiant fiscal attribué par l'administration fiscale à toute personne physique ou morale, qu'il s'agisse d'un individu ou d'une entreprise, afin de l'identifier et de suivre sa situation fiscale. Ce numéro est utilisé dans diverses transactions officielles, telles que les déclarations fiscales, l'émission de factures et les relations avec les administrations comme les douanes et les banques. Il constitue également une condition essentielle pour exercer toute activité commerciale ou professionnelle de manière légale. Ce système contribue ainsi à organiser les transactions financières et à renforcer la transparence au sein du système fiscal.

5.3.1. Procédure d'obtention du NIF

Etape 01 : Dépôt de la demande : le demandeur remplit le formulaire de demande d'immatriculation fiscale en ligne. Un accusé de réception portant le numéro de la demande est ensuite affiché à l'écran.

Etape 02 : Suivi de la demande : le demandeur peut suivre l'état d'avancement du traitement de sa demande via le lien « Suivre votre demande ».

Etape 03 : Impression de l'attestation d'immatriculation fiscale : le demandeur imprime son attestation à partir du lien dédié.

Etape 04 : Validation de l'attestation : le demandeur se présente au service de gestion compétent (inspection, CDI ou DGE) muni de l'accusé de réception et de l'attestation d'immatriculation. Si les informations sont correctes, le responsable appose son cachet et sa signature.

5.4. Présentation de la plateforme " Jibaya'tic "

Jibaya'tic est le nouveau portail de l'administration fiscale algérienne. Il offre les services de déclaration d'impôts & taxes à distance, déclinés dans un environnement qui assure simplicité, facilité et convivialité d'utilisation. Destiné aux contribuables relevant des nouvelles structures (DGE, CDI, CPI), ce portail est au sein d'un processus d'amélioration continu, un enrichissement fonctionnel et un élargissement des services. Pour cela, nous comptons sur la participation de nos contribuables pour lesquels un service d'écoute sera dédié.

A l'issue d'une procédure d'adhésion simplifiée aux services de Jibaya'tic, le contribuable se fera attribuer un accès à un espace privé et sécurisé où plusieurs services lui seront offerts :

- L'accès à ses données d'identification (raison sociale, adresse, coordonnées téléphoniques, etc.…).

- La possibilité d'une saisie assistée d'une déclaration d'impôts, avec calcul automatique et choix d'options sous forme de listes déroulantes. Ce service donne, en outre, l'assurance au contribuable d'une saisie conforme aux règles fiscales à jour. Il est également possible de mettre à jour une déclaration saisie et non encore transmise.

- Un dispositif de transmission des déclarations pour paiement avec un suivi continu sur tout l'exercice. Le portail offre également une documentation complète sur le système fiscal algérien, accessible à tous. Avantages Plus qu'une diversification de formules de déclaration

et de paiement d'impôts & taxes, Jibaya’tic recèle divers avantages pour le contribuable adhérent.

•Il est gratuit et simple d'accès avec une utilisation intuitive.

•Il est sécurisé avec une accessibilité et disponibilité maximales.

•Une aide conviviale accompagne la saisie, conformément aux règles fiscales à jour, ce qui prémunit d'erreurs de calculs et coquilles inhérentes à la procédure papier.

•L’ensemble des échanges et données du contribuable demeurent disponibles et accessibles dans son espace privé.

•Il offre une meilleure traçabilité et maîtrise des échanges avec l'Administration Fiscale, grâce à un suivi précis des déclarations envoyées.

•Il offre un tableau de bord sur les opérations effectuées.

6. Simulation de la mise en œuvre de la méthode EBIOS Risk Manager sur le portail « Jibaya’tic »

Atelier 1 : Cadrage et Socle de Sécurité

6.1. Cadrage de l’étude

6.1.1. Objectif de l’étude

L’objectif de cette étude est d’identifier et d’analyser les risques liés à la sécurité du portail public Jibaya’tic et de proposer des mesures à prendre pour garantir la confidentialité, l’intégrité et la disponibilité des données et des services offerts.

6.1.2. Contexte

Le système d’information JIBAYA’TIC est une solution, intégrée et centralisée, de type ERP (SAP TRM) élaborée conformément aux meilleures pratiques reconnues en gestion de la fiscalité et aux normes internationales applicables en comptabilité analytique. Il permet de numériser l’ensemble des processus et procédures fiscales de la DGI ainsi que la délivrance de services en lignes destinés aux contribuables.

a. **Durée des cycles :** le cycle stratégique et le cycle opérationnel sont d'un mois

b. **Contraintes** : le code général des impôts, la loi sur la protection des données personnelles (loi n° 18-07), la loi sur protection des personnes physiques dans le traitement des données à caractère personnel (loi n° 25 -11).et les contraintes imposées par la Direction générale des impôts (DGI)

6.1.3. Périmètre de l'étude

A- Périmètre métier

- **Piloter :**

- Définir les objectifs et assurer leur suivi.
- Effectuer des analyses.
- Faire évaluer les dispositions fiscales et réglementaires.
- Gérer les habilitations.

- **Gérer les relations avec les contribuables :**

- Accueillir et informer un contribuable en ligne.
- Authentifier et Accueillir le contribuable en ligne.
- Enregistrer et pris en charge le courrier et les courriels.
- Planifier les rendez-vous**.**

- **Gérer le dossier des contribuables :**

- Créer le dossier fiscal du contribuable.
- Habiliter les personnes représentant le contribuable.
- Attribuer les droits accès en ligne.
- Tenir et mettre à jour les sous dossiers en ligne.
- Gérer le fichier des contribuables.
- Gérer le fichier foncier.
- Préparer la clôture d'un dossier fiscal.
- Classer et archiver le dossier / accéder aux dossiers.

- **Gérer l'assiette :**

- Recevoir et enregistrer les déclarations.
- Relancer les contribuables défaillants.
- Opérer les régularisations.
- Gérer le régime des franchises et avantage fiscaux.

- **Liquider :**

- Enregistrer les paramètres de taxation.
- Effectuer la liquidation.
- Transférer le titre et le constater comptablement.

- **Encaisser et recouvrer :**

- Encaisser.
- Comptabiliser les produits.
- Relancer / poursuivre.
- Transférer les situations fiscales.

- **Contrôler :**

- Rechercher la matière imposable.
- Effectuer et contrôler et tenir le dossier de contrôle.
- Etablir les programmes de contrôle.

- **Gérer les recours et les contentieux :**

- Gérer les recours gracieux
- Gérer les contentieux
- Gérer les recours sur les contentieux

B- Périmètre technique

Le système comprend :

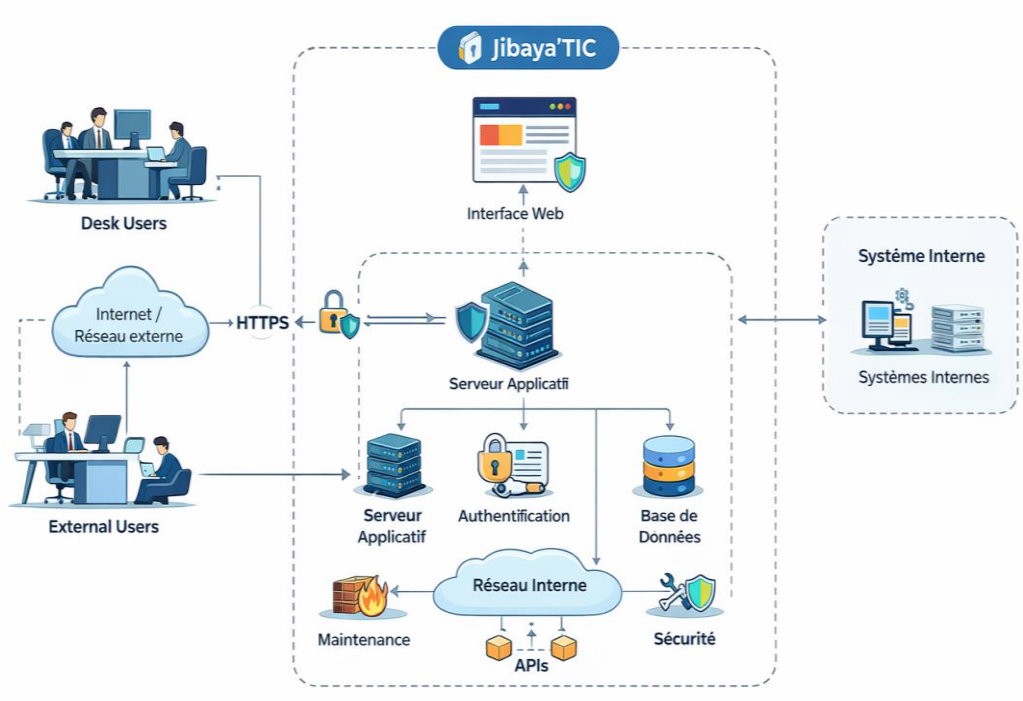
- Interface web (front-end).
- Serveurs applicatifs.
- Base de données.
- Système d'authentification
- Réseau et infrastructure.

Interconnexion avec systèmes internes :

- Interconnexion avec l'ERP Jibaya'tic (modules CRM, TRM, comptabilité).
- Interconnexion avec le système d'authentification centralisé (SSO/LDAP).

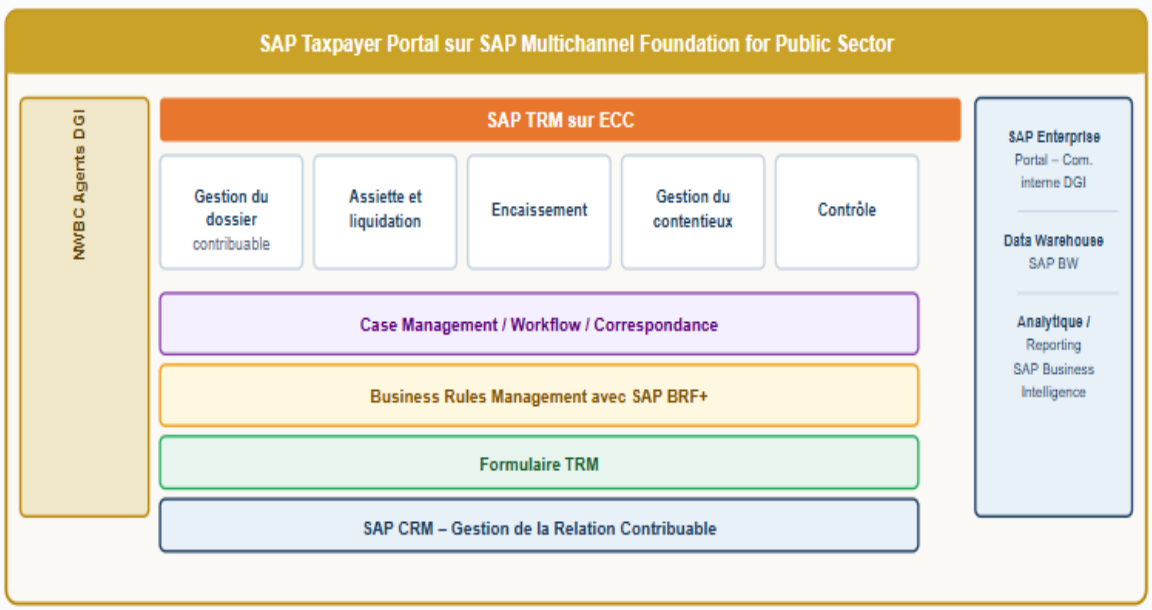
- Interconnexion avec la passerelle de paiement.

Figure14: Architecture fonctionnelle et sécurisée du portail « Jibaya'tic ».



Source : préparée par nous même à travers les document fournis par la DGI

Figure 15: la cartographie fonctionnelle du système d'information SI-Jibaya'tic.



Sources : le document fourni par la DGI

6.1.4. Acteurs et rôles

Concernant le portail Jibaya'tic, il existe plusieurs parties prenantes qui ont chacune un rôle spécifique. La première de ces parties prenantes est la direction des systèmes d'information qui gère le système et s'occupe des développements, maintenance, gestion des risques et l'application du plan de traitement des risques, le responsable de sécurité des système d'information qui occupe le rôle de décideur en matière de sécurité, les différents direction métier de la DGI qui sont responsable de chaque processus métier, Les contribuables, qui sont des citoyens, interagissent avec ce portail comme étant les derniers utilisateurs pour pouvoir effectuer leurs transactions administratives.

6.1.5. Valeurs métier (Biens essentiels)

Les valeurs métier représentent les éléments critiques à protéger et les biens supports sont les éléments techniques supportant les valeurs métier.

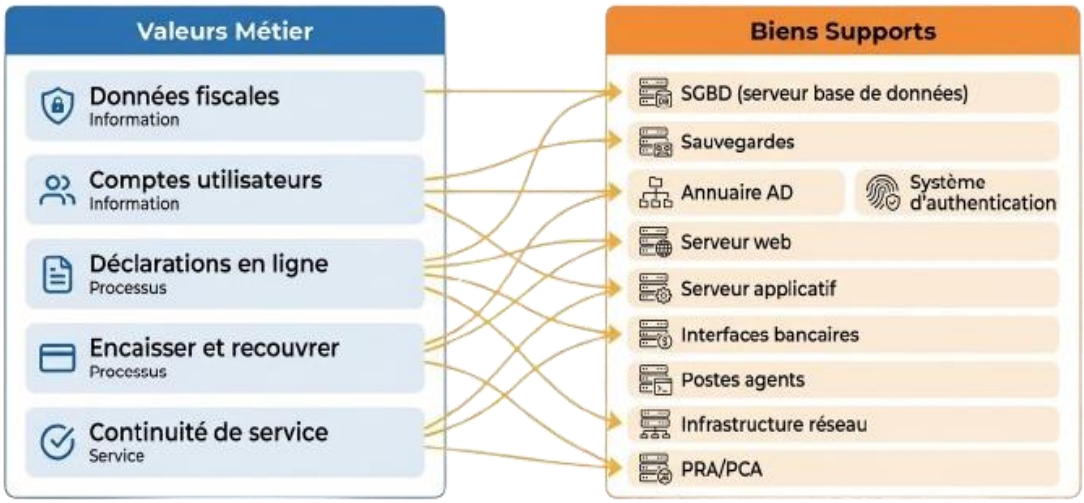
Tableau 4: Valeurs métier.

Valeur métier	Type	Description	Biens supports
Données fiscales	Information	Données sensibles des contribuables (identité, revenus, impôts, historiques)	SGBD (serveur base de données), sauvegardes
Comptes utilisateurs	Information	Données d'authentification et de gestion des accès (contribuables et agents)	Annuaire AD
Déclarations en ligne	Processus	Saisie, validation et soumission des déclarations fiscales via le portail	Serveur web, serveur applicatif
Encaisser et recouvrer	Processus	Traitement des paiements, suivi des encaissements et gestion des recettes fiscales	Serveur applicatif, interfaces bancaires, postes agents

Continuité de service	Service	Disponibilité du portail Jibaya'tic (télédéclaration, télépaiement)	Serveur web, serveur applicatif, serveur BD, infrastructure réseau, PRA/PCA

Source : préparée par nous même à travers les document fournis par la DGI

Figure 16: Relation entre la valeur métier du système Jibaya'tic et les bien supports correspondants.



Source : préparée par nous même à travers les document fournis par la DGI.

Ce schéma illustre la relation entre les valeurs métier du système Jibaya'tic et les biens supports techniques qui assurent leur fonctionnement.

6.1.6. Événements redoutés (ER) :

L'identification des événements redoutés permet de mesurer les conséquences potentielles des atteintes aux actifs critiques du système. Les résultats révèlent que les risques liés à la confidentialité, à l'intégrité et à la disponibilité des données présentent une gravité élevée, justifiant la mise en place de mesures de sécurité renforcées.

Tableau 5: Événements redoutés (ER).

Valeur métier	Événement redouté	Impact	Gravité
Données fiscales	- Accès non autorisé entraînant la divulgation massive des données fiscales des contribuables.	- Atteinte à la confidentialité des données personnelles et financières. - Perte de confiance des contribuables. - Risques juridiques et sanctions réglementaires.	G4
Déclarations fiscales en ligne	- Modification frauduleuse des déclarations soumises sans consentement des contribuables.	- Atteinte à l'intégrité des données fiscales. - Litiges avec les contribuables. - Impact juridique et administratif pour l'administration.	G4
Comptes utilisateurs	- Usurpation d'identité permettant un accès non autorisé aux comptes. - Modification non autorisée des habilitations permettant à un utilisateur d'obtenir des privilèges élevés.	- Atteinte à la confidentialité des comptes - Réalisation d'opérations frauduleuses - Accès aux fonctions critiques (suppression, modification, validation)	G3
Portail de téléservices (MCF / Jibaya'tic)	- Indisponibilité totale ou partielle du portail pendant une période prolongée.	- Atteinte à la disponibilité des services. - Interruption des télédéclarations et télépaiements. - Non-respect des délais légaux.	G4

Données fiscales base de données	- Suppression accidentelle ou malveillante des données sans possibilité de restauration rapide.	- Perte d'intégrité et de disponibilité des données. - Perturbation majeure des activités fiscales. - Impact financier et organisationnel.	G4

Source : préparée par nous même à travers les document fournis par la DGI

Échelle de gravité :

G1 : Mineure

G2 : Significative

G3 : Grave

G4 : Critique

6.1.7. Besoins de sécurité

Le système doit garantir :

- **Confidentialité :** protection des données sensibles
- **Intégrité :** exactitude des informations
- **Disponibilité :** accès permanent
- **Authenticité :** vérification des utilisateurs
- **Traçabilité :** suivi des actions

6.1.8. Analyse des écarts

Les principaux écarts identifiés sont :

- Partage de comptes administrateurs pour certains modules.
- Gestion insuffisante des habilitations sur les environnements SAP, liée à la règle 8 :« Identifier nominativement chaque personne accédant au système ».
- Absence d'audit régulier

Conclusion de la 1ere atelier

L'atelier numéro 1 a servi à déterminer le cadre du projet, à analyser les composantes importantes du système et également les risques initiaux importants.

Jibaya’tic possède une importance stratégique par le fait qu'il manipule des informations très sensibles et qu'il est exposé sur internet.

Les résultats seront utilisés dans la suite des ateliers pour identifier les sources de risque et construire des scénarios d'attaque.

Atelier 2 : Sources de Risque

6.2. Objectif de l’atelier

Le but de cette séance est donc de mettre en évidence les sources de menace qui peuvent menacer l’infrastructure Jibaya’tic, et des objectifs qui pourraient être visés par celles-ci.

Cette démarche cherche donc à répondre à la question suivante :

Quelques adversaires peuvent attaquer ce système et pourquoi ?

Ceci nous permettra de faire la transition entre notre approche défensive (séance 1) et notre approche offensive.

6.2.1. Participants à l’atelier

Cet atelier mobilise plusieurs acteurs ayant des compétences complémentaires, notamment :

- Les responsables métiers, connaissant les processus liés au portail
- L’équipe technique (développement et systèmes)
- Les responsables de la sécurité des systèmes d’information
- Éventuellement un expert en cybersécurité ou en analyse de la menace

La participation de ces différents profils permet d’avoir une vision globale et réaliste des menaces potentielles.

6.2.2. Données de sortie

À l’issue de cet atelier, les résultats attendus sont :

- Une liste de sources de risque identifiées
- Une liste des objectifs visés par ces sources
- Une sélection des couples source de risque / objectif visé (SR/OV) les plus pertinents

- Une représentation synthétique des sources de risque (cartographie)

6.2.3. Sources de risque / Objectifs visés (SR/OV)

Ce tableau présente les principales sources de risque susceptibles d'affecter le portail Jibaya'tic ainsi que leurs objectifs. Il met en évidence la diversité des menaces, qu'elles soient internes ou externes, et démontre que les cybercriminels ainsi que les acteurs internes malveillants représentent des sources de risque particulièrement préoccupantes pour la DGI.

Tableau 6: Sources de risque / Objectifs visés

Source de risque (SR)	**Objectif visé (OV)**
Cybercriminel	- Accéder illégalement aux données fiscales afin de les exploiter ou les revendre à des fins financières. - Bloquer l'accès au portail (attaque de type DDoS ou ransomware) afin d'exiger une rançon.
Hacktiviste	- Perturber le fonctionnement du portail pour exprimer une opposition idéologique ou politique. - Divulguer des informations sensibles pour nuire à l'image de l'administration. - Défigurer le portail pour afficher des messages militants.
Employé interne malveillant	- Abuser de ses privilèges pour consulter, modifier ou extraire des données sensibles - Altérer des informations fiscales à des fins personnelles ou frauduleuses
Utilisateur malveillant	- Créer de faux comptes ou exploiter des failles pour accéder à des services non autorisés
Attaquant opportuniste	- Exploiter des vulnérabilités techniques du système pour obtenir un accès non autorisé

Prestataire / tiers	- Accéder à des données sensibles dans le cadre d'interventions techniques - Introduire involontairement des vulnérabilités ou des erreurs de configuration - Abuser d'un accès distant insuffisamment contrôlé
Concurrent (cas indirect)	- Tenter d'obtenir des informations stratégiques liées au système ou à son fonctionnement

Source : préparée par nous même à travers les document fournis par la DGI

6.2.4. Identification des sources de risque et des objectifs visés :

Dans cette étape, il s'agit d'identifier les différentes sources de risque pouvant cibler le portail Jibaya'tic, ainsi que leurs intentions.

Les sources de risque peuvent être internes ou externes, intentionnelles ou accidentelles. Elles sont généralement caractérisées par leur nature, leurs capacités et leurs motivations.

Parmi les sources de risque possibles dans le contexte du portail, on peut citer :

- Les cybercriminels cherchant un gain financier.
- Les hacktivistes motivés par des causes idéologiques.
- Les utilisateurs malveillants ou négligents.
- Les employés internes ayant des accès privilégiés.
- Les attaquants opportunistes exploitant des vulnérabilités.
- Prestataire / tiers profite de ces missions temporaires volontairement ou involontairement.
- Concurrent (cas indirect) ne s'agit pas d'une attaque directe contre le portail, mais d'un concurrent cherchant à obtenir des avantages stratégiques via le système.

Chaque source de risque est associée à un ou plusieurs objectifs visés, tels que :

- Le vol de données fiscales.
- La perturbation du service.

- La modification des informations.
- L'accès non autorisé aux comptes.
- La dégradation de l'image de l'administration.
- Confidentialité (obtenir des informations sans autorisation) et Atteinte indirecte à l'avantage concurrentiel et à la réputation

Donc L'analyse détaillée des sources de risque permet de mieux comprendre leurs caractéristiques, leurs motivations et leurs intentions. Cette étape contribue à affiner l'évaluation des menaces et facilite l'identification des scénarios de risque les plus plausibles dans l'environnement du portail Jibaya'tic.

Tableau 7: détaillé source de risqué/Objectifs visés (SR/OV).

Source de risque (SR)	**Type**	**Description**	**Objectif visé (OV)**
Cybercriminel	Externe	Individu ou groupe organisé cherchant un gain financier à travers des activités illégales en ligne	- Accéder aux données fiscales des utilisateurs afin de les exploiter, les revendre ou effectuer du chantage. - Bloquer l'accès au portail et perturber les services afin d'exiger une rançon.
Hacktiviste	Externe	Groupe motivé par des idéologies politiques ou sociales visant à dénoncer ou perturber un système public	- Rendre le portail indisponible afin de protester ou attirer l'attention médiatique. - Divulguer des données internes pour nuire à l'image de l'administration fiscale.
Employé interne malveillant	Interne	Personne disposant d'un accès légitime au système et l'utilisant à des fins personnelles ou malveillantes	- Accéder, modifier ou supprimer des données sans autorisation en abusant de ses privilèges.

Employé interne négligent	Interne	Utilisateur interne manquant de vigilance ou de formation en sécurité	- Provoquer une fuite ou une altération de données suite à une mauvaise manipulation ou erreur humaine.
Utilisateur malveillant	Externe	Utilisateur cherchant à exploiter le système à des fins frauduleuses	- Créer de faux comptes ou contourner les mécanismes de sécurité pour accéder à des services non autorisés.
Attaquant opportuniste	Externe	Individu exploitant automatiquement des vulnérabilités connues sans ciblage spécifique	- Exploiter une faille du système pour obtenir un accès non autorisé ou injecter du code malveillant.
Prestataire / tiers	Externe	Sous-traitant, fournisseur ou partenaire disposant d'un accès partiel ou total aux systèmes, infrastructures ou données de l'organisme dans le cadre d'une relation contractuelle.	- Introduire intentionnellement ou accidentellement un code malveillant lors d'une intervention sur le système (supply chain attack). - Provoquer une interruption de service suite à une mauvaise configuration ou une défaillance non maîtrisée. - Exfiltrer des informations sensibles (données contribuables, paramètres techniques) vers des tiers non autorisés.
Concurrent (cas indirect)	Externe	Acteur externe intéressé par les systèmes ou les données pour des raisons stratégiques	- Obtenir des informations techniques ou organisationnelles pouvant donner un avantage indirect.

Source : préparée par nous même à travers les document fournis par la DGI

6.2.5. Évaluation de la pertinence des couples SR/OV

Après l'identification des couples source de risque / objectif visé (SR/OV), il est nécessaire d'évaluer leur pertinence afin de retenir uniquement les menaces les plus réalistes et impactantes pour le système Jibaya'tic.

Cette évaluation repose sur trois critères principaux :

- **Motivation** : niveau d'intérêt de la source de risque à atteindre son objectif
- **Ressources** : moyens techniques, financiers et humains disponibles
- **Activité** : niveau d'activité de la menace dans le contexte étudié

Tableau 8: d'évaluation des couples SR/OV.

SR/OV	Motivation	Ressources	Activité	Pertinence
Cybercriminel	Élevée	Élevées	Élevée	Élevée
Hacktiviste	Moyenne	Moyennes	Moyenne	Moyenne
Employé interne	Élevée	Moyennes	Moyenne	Élevée
Utilisateur malveillant	Moyenne	Faibles	Élevée	Moyenne
Attaquant opportuniste	Moyenne	Faibles	Élevée	Moyenne
Concurrent	Faible	Moyennes	Faible	Faible
Prestataire / tiers	Moyennes	Moyennes	Faible	Moyennes

Source : préparée par nous même à travers les document fournis par la DGI

6.2.6. Sélection des couples SR/OV retenus

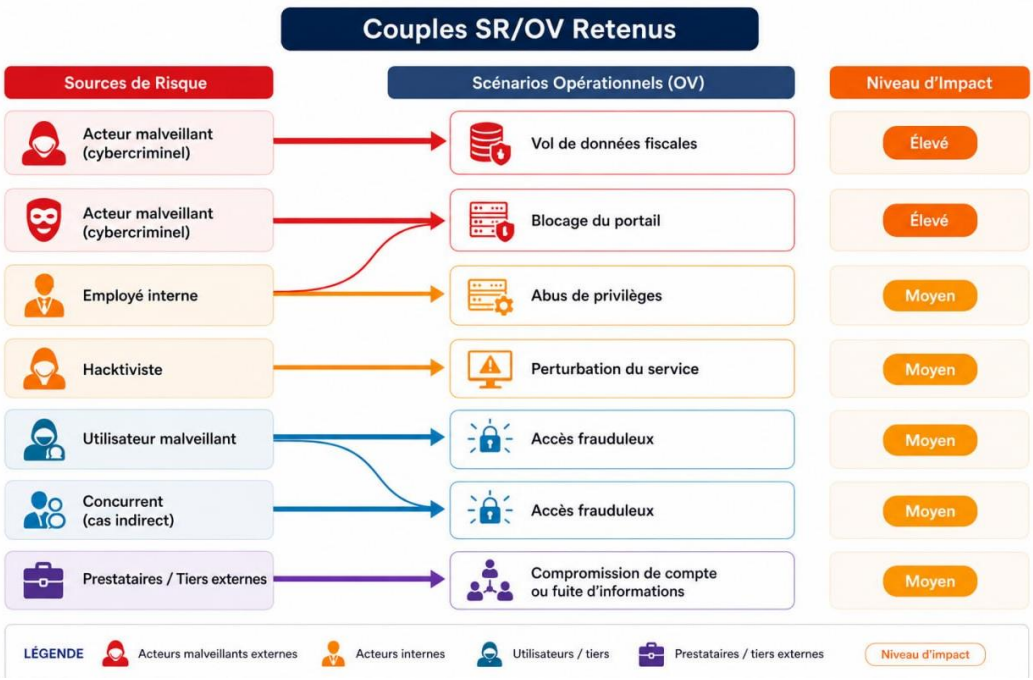
Sur la base de l'évaluation précédente, seuls les couples présentant un niveau de pertinence élevé ou moyen sont retenus pour la suite de l'analyse.

Les couples sélectionnés sont les suivants :

- Cybercriminel / Vol de données fiscales
- Cybercriminel / Blocage du portail
- Employé interne / Abus de privilèges
- Hacktiviste / Perturbation du service
- Utilisateur malveillant / Accès frauduleux
- Prestataire / Mauvaise configuration

La cartographie met en évidence les couples *Source de Risque / Objectif Visé* présentant le niveau de criticité le plus élevé pour le portail Jibaya'tic. Elle permet d'identifier les menaces les plus plausibles et les plus impactantes, facilitant ainsi la priorisation des actions de sécurité. Les résultats montrent que certaines sources de risque disposent à la fois de la capacité et de la motivation nécessaires pour compromettre les actifs critiques du système, ce qui justifie une vigilance particulière et la mise en œuvre de mesures de protection adaptées.

Figure 17: Ces couples représentent les menaces les plus crédibles et les plus critiques pour le portail Jibaya'tic.



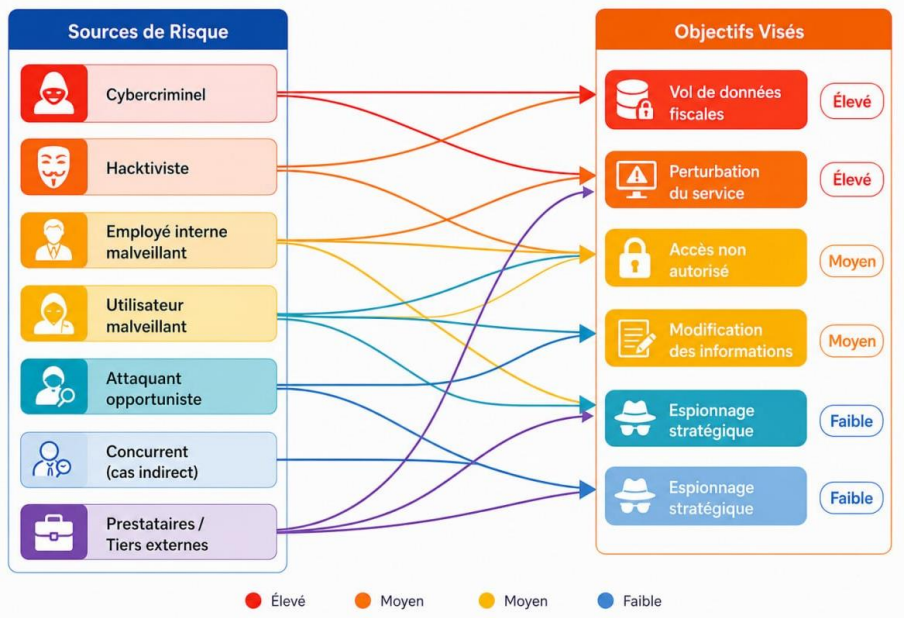
Source : préparée par nous même à travers les document fournis par la DGI

6.2.7. Cartographie des sources de risque

La cartographie des sources de risque permet de représenter visuellement les menaces en fonction de leur niveau de pertinence.

Elle met en évidence les sources de risque les plus critiques, facilitant ainsi la prise de décision et la priorisation des actions de sécurité.

Figure 18: Cartographie des sources de risque



Source : préparée par nous même à travers les document fournis par la DGI

6.2.8. Conclusion du 2eme atelier

L'atelier 2 a permis d'identifier et de caractériser les principales sources de risque pesant sur le portail Jibaya'tic, ainsi que les objectifs qu'elles cherchent à atteindre.

L'évaluation des couples SR/OV a permis de retenir un nombre limité de scénarios pertinents, assurant ainsi une analyse ciblée et efficace pour la suite de la méthode.

Les résultats obtenus serviront de base pour l'atelier 3, qui consistera à construire des scénarios stratégiques en s'appuyant sur les couples sélectionnés.

Atelier 3 : Scénarios stratégiques

6.3. Objectif de l'atelier

Le but de cette activité est de faire l'analyse de l'écosystème du portail Jibaya'tic pour déterminer quels acteurs peuvent être des vecteurs d'attaques et de créer ensuite des scénarios stratégiques qui décrivent les chemins d'attaques potentielles.

Le principe est d'observer comment la source de menace peut profiter des interactions du système avec son environnement pour réaliser ses ambitions.

On passe ainsi de l'étape des menaces à celle des scénarios d'attaques en haute altitude grâce à cette activité.

6.3.1. Participants à l'atelier

Pour que cet atelier soit efficace, il faut la participation de multiples intervenants pour qu'une analyse complète de l'écosystème puisse être effectuée :

- Les intervenants métier pour identifier les interactions entre partenaires.
- Les intervenants techniques pour comprendre le flux et les interconnexions.
- Les intervenants en sécurité des systèmes d'informations.
- Les intervenants concernant les relations contractuelles (fournisseur prestataires).

Le nombre important de participants permet ainsi une meilleure identification des éléments d'exposition aux parties prenantes.

6.3.2. Données d'entrée

L'approche de ces travaux est basée sur les résultats obtenus lors de l'atelier précédent qui comprennent entre autres :

- Les valeurs métier définies lors de l'atelier n° 1.
- Les supports de valeur liés.
- Les évènements redoutables et leur niveau d'importance.
- Les SR/OV choisis lors de l'atelier n° 2.
- La connaissance du système et de son environnement.

Cela permet d'établir un portrait global du système et de son écosystème.

6.3.3. Données de sortie

La sortie de cet atelier donne une vision structurée du milieu au sein duquel se déroule le fonctionnement du portail Jibaya'tic. Cette vision aide à mettre en lumière l'interaction du système avec les entités extérieures et intérieures et leurs points potentiels de vulnérabilité.

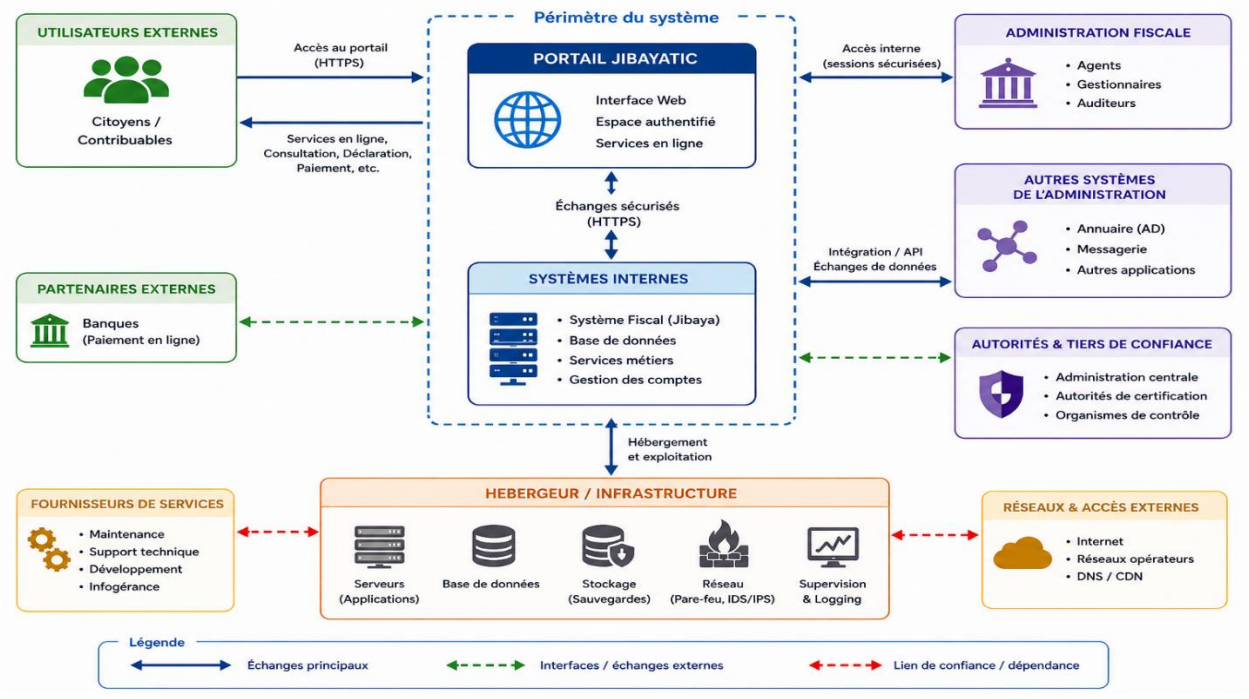
Il s'agit des informations obtenues qui sont ensuite utilisées pour élaborer les scénarios stratégiques, particulièrement grâce à l'analyse des parties prenantes qui peuvent servir de vecteur d'attaque.

6.3.4. Cartographie de l'écosystème

La cartographie de l'écosystème consiste à représenter de manière globale les relations entre le portail Jibaya'tic et les différents acteurs avec lesquels il interagit. L'objectif n'est pas de détailler les aspects techniques internes, mais plutôt de comprendre comment le système s'insère dans son environnement et dépend d'autres entités pour fonctionner.

Dans le cas étudié, le portail est en interaction avec plusieurs éléments externes et internes, notamment les utilisateurs (citoyens), les systèmes internes de l'administration fiscale, ainsi que les prestataires techniques comme l'hébergement ou les services de sécurité. Ces relations constituent des points de contact pouvant être exploités en cas de vulnérabilité ou de faiblesse du système.

Figure 19: cartographie de l'écosystème du portail Jibaya'tic.



Source : préparée par nous même à travers les document fournis par la DGI

6.3.5. Identification des parties prenantes

Le processus d'identification des parties prenantes permet d'énumérer les organisations qui entrent en contact avec le portail, tant de manière directe qu'indirecte. Ceci est crucial, car tout lien avec une entité interne ou externe pourrait servir de voie d'entrée pour un potentiel assaut.

En outre, il y a une division des parties prenantes internes et externes, où les premières incluent l'administration fiscale et les techniciens, tandis que les secondes sont constituées des clients ou des fournisseurs.

Tableau 9: détaillé Parties prenantes du portail Jibaya'tic.

Partie prenante	Type	Rôle	Interaction avec le système
Administration fiscale	Interne	Propriétaire du système et responsable métier	Définit les règles, accède au système interne et supervise les opérations
Équipe IT	Interne	Développement et maintenance	Gère l'infrastructure, les mises à jour et le bon fonctionnement technique
Équipe sécurité	Interne	Gestion de la sécurité	Met en place les mesures de sécurité et surveille les incidents
Contribuable	Externe	Utilisateurs finaux	Accèdent au portail pour consulter et effectuer des démarches fiscales
Hébergeur	Externe	Fournisseur d'infrastructure	Héberge les serveurs et assure la disponibilité du système et le sécurité physique
ERP Jibaya'tic (CRM, TRM…)	Interne	Système métier central	Reçoit les déclarations et paiements soumis via le portail

Base de données centrale	Interne	Stockage des données	Stocke et restitue toutes les données fiscales du portail
Système d'authentification (SSO/LDAP)	Interne	Contrôle d'accès	Vérifie l'identité des utilisateurs et agents à la connexion
Fournisseurs de services	Externe	Support technique	Assurent la maintenance, le support ou des services spécifiques
Partenaires externes	Externe	Services complémentaires	Interagissent avec le système (paiement, authentification, etc.)
Réseaux externes (Internet)	Externe	Canal de communication	Permettent l'accès des utilisateurs au portail

Source : préparée par nous même à travers les document fournis par la DGI.

6.3.6. Évaluation de la dangerosité des parties prenantes

Une fois ces parties prenantes identifiées, une évaluation de leur dangerosité doit être effectuée. L'idée de dangerosité ici ne signifie pas que cette partie prenante est hostile à l'entreprise, mais elle est utilisable par une source de risque pour réaliser un certain but.

Il existe des critères d'évaluation, entre autres : le degré d'accès aux systèmes, le degré d'exposition et la dépendance de ce portail à l'égard de la partie prenante. Par conséquent, si cette partie prenante dispose d'un accès spécial ou utilise des informations spéciales, sa dangerosité est plus élevée.

Tableau 10: Évaluation de la dangerosité des parties prenantes du système d'information.

Partie prenante	Accès au système	Niveau d'exposition	Dépendance du système	Niveau de sécurité	Dangerosité
Administration fiscale	Élevé	Faible	Élevée	Élevé	Moyen
Équipe IT	Élevé	Moyen	Élevée	Moyen	Élevé
Équipe sécurité	Élevé	Faible	Moyenne	Élevé	Faible
Contribuable	Moyen	Élevé	Élevée	Faible	Élevé
Hébergeur	Élevé	Moyen	Élevée	Moyen	Élevé
ERP Jibaya'tic (CRM, TRM…)	Élevé	Faible	Élevée	Moyen	Élevé
Base de données centrale	Élevé	Faible	Élevée	Moyen	Élevé
Système d'authentification (SSO/LDAP)	Élevé	Faible	Élevée	Moyen	Élevé
Fournisseurs de services	Moyen	Moyen	Moyenne	Faible	Moyen

Partenaires externes	Moyen	Moyen	Moyenne	Moyen	Moyen
Réseaux externes (Internet)	Faible	Élevé	Élevée	Faible	Élevé

Source : préparée par nous même à travers les document fournis par la DGI

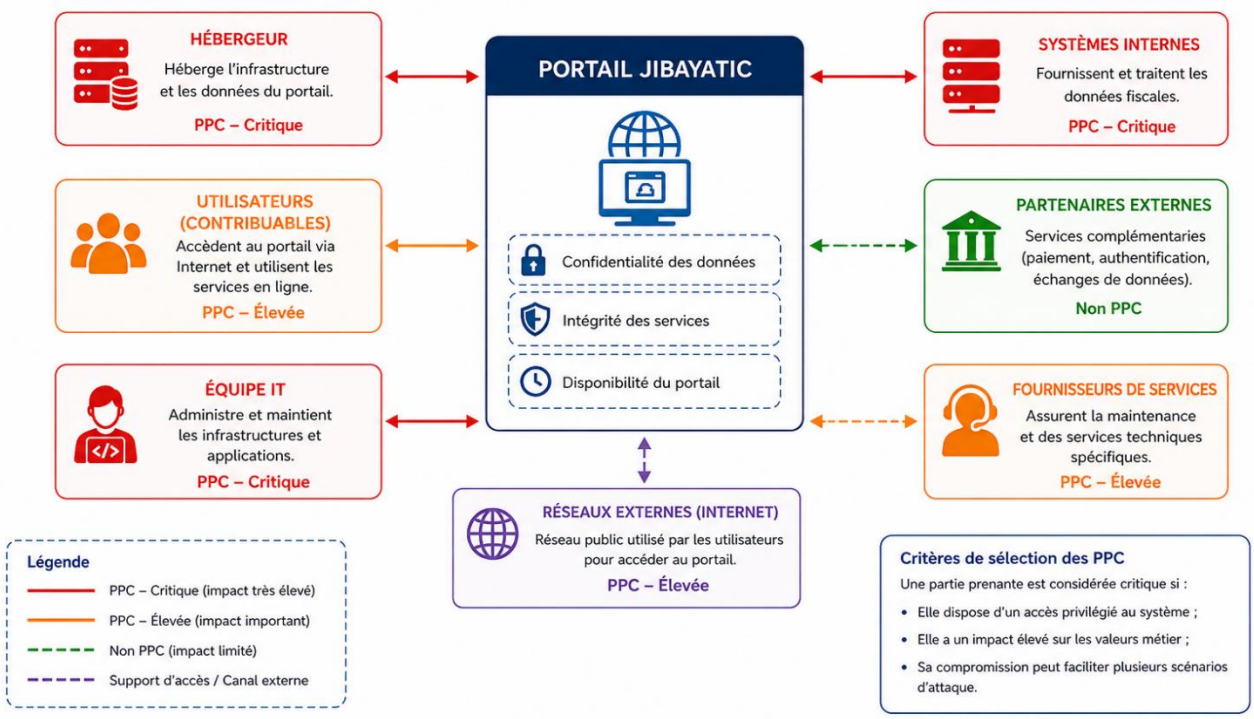
6.3.7. Sélection des parties prenantes critiques (PPC)

Compte tenu de l'évaluation précédente, les parties prenantes ayant le degré d'hostilité le plus élevé sont classées comme parties prenantes critiques. Elles servent de point d'entrée potentiel qui peut être utilisé pour mettre en œuvre les scénarios d'attaque.

Par exemple, au regard du portail Jibaya'tic, l'hébergeur, le système interne interconnecté et même l'utilisateur peuvent faire office de parties prenantes critiques pour leur degré d'exposition.

Le choix de ces parties prenantes permet d'étudier les vecteurs d'attaques qui ont un réel intérêt dans le cours de l'étude.

Figure 20:partie prenantes critiques (PPC) du portail Jibaya'tic



Source : préparée par nous même à travers les document fournis par la DGI

6.3.8. Construction des scénarios stratégiques

La construction des scénarios stratégiques consiste à décrire, à un niveau global, les chemins d'attaque qu'une source de risque pourrait emprunter pour atteindre son objectif visé, en exploitant l'écosystème du portail Jibaya'tic.

Chaque scénario repose sur un couple SR/OV retenu lors de l'atelier 2 et intègre une ou plusieurs parties prenantes critiques identifiées précédemment. L'objectif est de comprendre comment un attaquant peut contourner les défenses du système en passant par des entités externes ou internes.

Dans ce contexte, un scénario stratégique ne détaille pas les aspects techniques, mais décrit plutôt la logique générale de l'attaque et les relations exploitées.

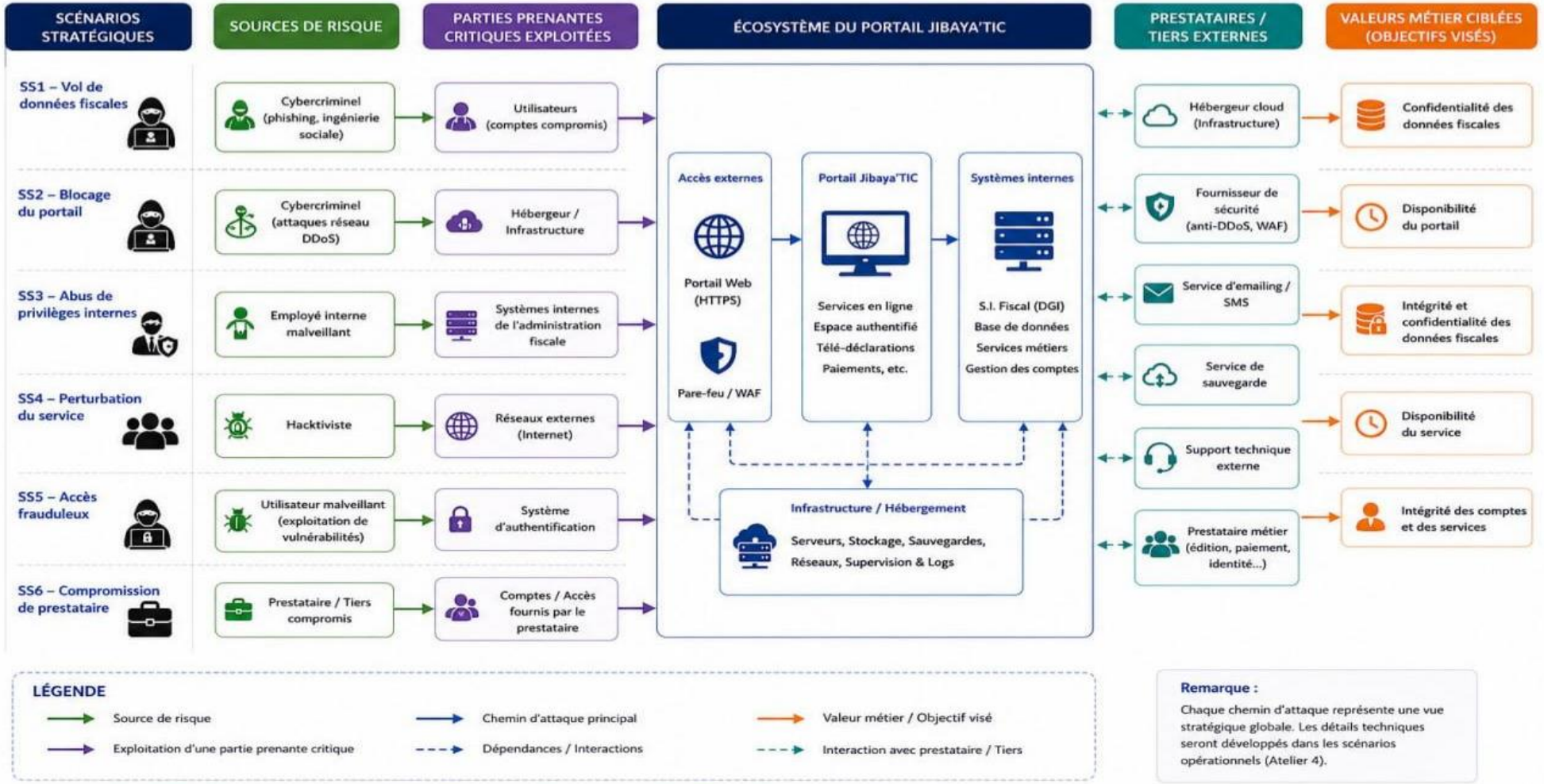
Tableau 11: Identification et analyse des scénarios de risques stratégiques

ID	Source de risque	Objectif visé	Partie prenante critique exploitée	Valeur métier ciblée	Scénario stratégique
SS1	Cybercriminel	Vol de données fiscales	Utilisateurs (comptes compromis)	Données fiscales	Un cybercriminel compromet des comptes utilisateurs via des techniques de phishing afin d'accéder aux données fiscales sensibles disponibles sur le portail
SS2	Cybercriminel	Blocage du portail	Hébergeur / infrastructure	Disponibilité du portail	Un attaquant cible l'infrastructure d'hébergement à travers une attaque de type DDoS pour rendre le portail indisponible
SS3	Employé interne malveillant	Abus de privilèges	Systèmes internes	Données fiscales	Un employé disposant d'un accès privilégié exploite les systèmes internes pour consulter ou extraire des données sensibles sans

					autorisation
SS4	Hacktiviste	Perturbation du service	Réseaux externes (Internet)	Disponibilité du portail	Un groupe hacktiviste lance des actions coordonnées visant à perturber le fonctionnement du portail pour des raisons idéologiques
SS5	Utilisateur malveillant	Accès frauduleux	Système d'authentification	Comptes utilisateurs	Un utilisateur exploite une faille dans le système d'authentification pour accéder à des comptes ou services non autorisés
SS6	Prestataire /tiers	Fuite ou compromission de données	Services externalisés /accès fournisseur	Données fiscales	Un prestataire disposant d'un accès au SI (maintenance, hébergement ou support) est compromis ou agit de manière malveillante, entraînant une fuite ou une altération des données fiscales

Source : préparée par nous même à travers les document fournis par la DGI

Figure 21: chemins d'attaque stratégiques Jibaya'tic.



Source : préparée par nous même à travers les document fournis par la DGI

6.3.9. Évaluation de la gravité des scénarios stratégiques

Après avoir réalisé les scénarios, le premier point à examiner est leur gravité. La gravité fait référence au niveau de danger que ce scénario pourrait causer pour les valeurs métier du système.

Pour évaluer la gravité, on prend en compte tous les risques retenus lors de la tenue de l'atelier 1. Dans ce cadre, toute gravité attachée à un scénario stratégique est due à son impact sur la confidentialité, intégrité et disponibilité de l'information. Ainsi, les scénarios qui concernent des informations sensibles ou entrainent une panne de service sont jugés comme les plus graves.

6.3.10. Mesures de sécurité liées à l'écosystème

Le processus d'analyse des scénarios stratégiques nous aidera à identifier certaines mesures de sécurité qui doivent être mises en œuvre à l'échelle de l'écosystème.

Il peut s'agir par exemple de renforcer le contrôle d'accès, de protéger les communications avec les partenaires, mais aussi de surveiller activement les comportements douteux.

Ces mesures viennent s'ajouter à la base de sécurité établie lors du workshop 1 et seront développées dans les workshops qui suivront.

Tableau 12: Mesures de sécurité associées aux scénarios de risques identifiés.

Scénario stratégique	Partie prenante concernée	Mesure de sécurité	Description
SS1 – Vol de données fiscales	Utilisateurs	- Authentification multi-facteurs (MFA) - Sensibilisation à la sécurité	- Renforcer l'authentification des utilisateurs afin de réduire le risque de compromission des comptes. - Former les utilisateurs aux risques de phishing et d'ingénierie sociale.
SS2 – Blocage du portail	Hébergeur / Infrastructure	- Protection anti-DDoS - Redondance des infrastructures	- Mettre en place des solutions de mitigation contre les attaques par déni de service. - Assurer la continuité du service via des

			mécanismes de haute disponibilité.
SS3 – Abus de privilèges	Équipe interne / SI où Systèmes internes	- Gestion des accès (IAM) - Journalisation et audit	- Appliquer le principe du moindre privilège et contrôler les accès. - Mettre en place un suivi des actions pour détecter les comportements anormaux.
SS4 – Perturbation du service	Réseaux externes / Infrastructure	- Filtrage réseau (Firewall / WAF) - Supervision en temps réel	- Contrôler et filtrer le trafic entrant pour limiter les attaques. - Détecter rapidement les anomalies et réagir efficacement.
SS5 – Accès frauduleux	Système d'authentification / Application	-Renforcement des contrôles d'accès - Tests de sécurité réguliers	- Implémenter des mécanismes de validation renforcée des accès. - Identifier et corriger les vulnérabilités applicatives.

Source : préparée par nous même à travers les document fournis par la DGI.

6.3.11. Conclusion du 3eme atelier

Avec le troisième atelier, il fut possible de comprendre l'écosystème du portail Jibaya'tic, ainsi qu'identifier les principaux acteurs qui peuvent être utilisés comme vecteurs d'attaque.

La construction de ces scénarios stratégiques nous a aidé à avoir une vision générale de tous les moyens d'attaques, en mettant particulièrement en évidence les interrelations importantes du système avec son environnement.

L'évaluation de l'intensité des scénarios nous a permis d'établir un ordre de risque, ainsi que de prendre certaines mesures de sécurité visant à protéger notre système.

Ces conclusions de l'atelier 3 forment le fondement de notre atelier 4.

Atelier 4 : Scénarios Opérationnel

6.4. Objectif de l’atelier

La finalité de cette session est la transformation de ces scenarii stratégies en scenarii opérationnels. Le but est ici d'illustrer par des faits concrets les modalités de fonctionnement qui pourrait suivre une menace dans son intention de faire une attaque sur le portail Jibaya’tic.

Dans cette phase, il n'y aura pas une approche stratégique telle que dans l'atelier précèdent, mais une approche technique ou les vulnérabilités exploitable, les points d'accès et les étapes d'attaques sont déterminées afin de savoir comment ce scenario pourrait vraiment se passer.

6.4.1. Participants à l’atelier

Cet atelier nécessite une forte implication des profils techniques, en particulier ceux ayant une connaissance approfondie du système et de ses mécanismes de sécurité.

- Les équipes IT interviennent pour détailler l’architecture technique et les point d’accès possibles.
- Les responsables sécurité analysent les vulnérabilités et les techniques d’attaque potentielles.
- Les architectes systèmes apportent une vision globale des interactions techniques.
- Des experts en cybersécurité peuvent être mobilisés pour enrichir l’analyse des modes opératoires.

Cette diversité permet de produire des scénarios réalistes et techniquement cohérents.

6.4.2. Données d’entrée

Les scénarios opérationnels s’appuient directement sur les résultats des ateliers précédents, notamment les scénarios stratégiques et les éléments techniques du système.

- Les scénarios stratégiques retenus (atelier 3).
- Les parties prenantes critiques (PPC).
- Les valeurs métier ciblées.
- Les biens supports identifiés (serveurs, base de données, authentification…).
- Les événements redoutés et leur gravité.

Ces données permettent de passer d'une vision globale à une description technique détaillée des attaques possibles.

6.4.3. Données de sortie

À l'issue de cet atelier, les résultats obtenus permettent de formaliser une vision précise des scénarios d'attaque.

- Une liste structurée de scénarios opérationnels.
- Une description détaillée des chemins d'attaque.
- Une estimation de la vraisemblance de chaque scénario.
- Une base solide pour l'évaluation des risques (atelier 5).

Tableau 13: détaillé Synthèse des scénarios opérationnels.

ID	Scénario stratégique associé	Scénario opérationnel	Point d'entrée	Biens supports ciblés	Impact principal
SO1	SS1 – Vol de données fiscales	Compromission de comptes utilisateurs via phishing permettant l'accès aux données fiscales	Interface web (authentification)	Système d'authentification, base de données	Atteinte à la confidentialité des données
SO2	SS2 – Blocage du portail	Attaque DDoS ciblant les serveurs pour saturer les ressources et rendre le service indisponible	Réseau externe (Internet)	Serveurs, infrastructure réseau	Atteinte à la disponibilité du service
SO3	SS3 – Abus de privilèges	Utilisation abusive d'un compte interne avec privilèges élevés pour extraire des données sensibles	Accès interne (SI)	Systèmes internes, base de données	Atteinte à la confidentialité et à l'intégrité
SO4	SS4 – Perturbation du service	Injection de requêtes malveillantes visant à perturber le fonctionnement de	Interface web / API	Serveur applicatif, backend	Dégradation du service

		l'application			
SO5	SS5 – Accès frauduleux	Exploitation d'une vulnérabilité dans le système d'authentification pour accéder à des comptes	Système d'authentification	Application, gestion des comptes	Accès non autorisé

Source : préparée par nous même à travers les document fournis par la DGI

Ce tableau présente une synthèse des principaux scénarios opérationnels identifiés pour le portail Jibaya'tic, en précisant pour chacun le point d'entrée, les biens supports ciblés ainsi que l'impact potentiel sur le système. Il met en évidence que les attaques de type phishing, les abus de privilèges internes et les attaques DDoS constituent des menaces majeures susceptibles de compromettre la confidentialité, l'intégrité ou la disponibilité des données et des services. Cette analyse permet d'orienter les efforts de sécurité vers les scénarios les plus critiques et de préparer l'évaluation détaillée des risques dans les étapes suivantes de la méthode EBIOS RM.

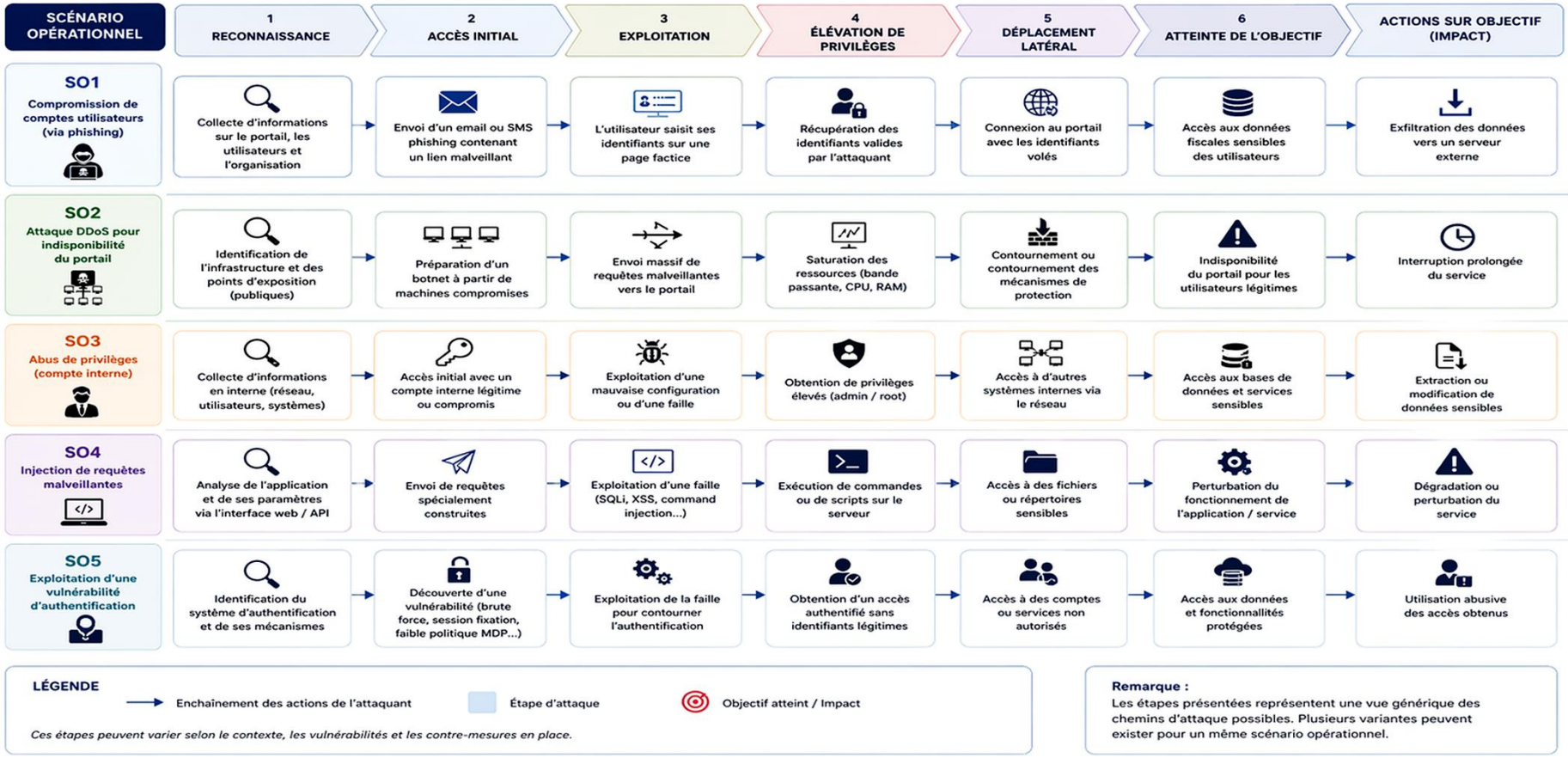
6.4.4. Identification des scénarios opérationnels

Définition des scénarios opérationnels : La deuxième phase consiste à énumérer tous les chemins d'attaque possibles à partir de chaque scénario stratégique, c'est-à-dire à définir une ou plusieurs séquences d'actions que l'attaquant doit mettre en œuvre pour parvenir à son but.

Pour cette phase, il convient d'utiliser une pensée systémique de l'attaque et de décrire étape par étape la progression de l'attaquant dans sa démarche d'intrusion, de la phase de l'entrée au passage à l'acte et aux conséquences de l'attaque.

La variété des points de départ et de fin, et des chemins de réalisation des attaques, permet de générer des scénarios de faits réels et techniques.

Figure 22:étapes d'attaque – scénario opérationnels



Source : préparée par nous même à travers les document fournis par la DGI

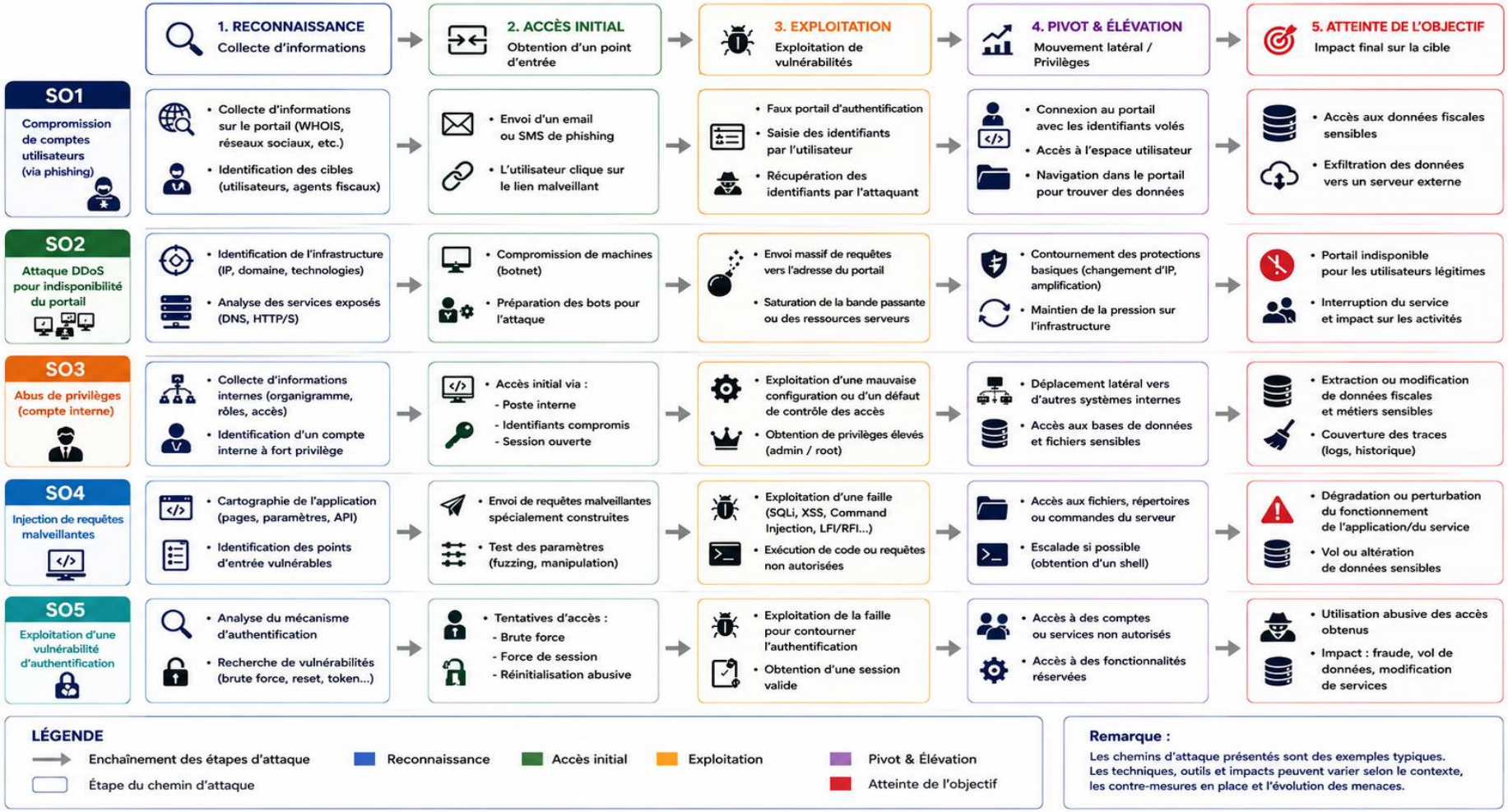
6.4.5. Description des scénarios (chemins d’attaque détaillés)

Ce point concerne la description précise de chaque scenario opérationnel. C'est la description de la succession des actions entreprises par le pirate dans la tentative d'attaquer le système.

Les scénarios sont construits par un point d'entrée avec différentes étapes qui vont de l'accès au but final atteint. À travers cette description sera possible d'identifier les failles utilisées par le pirate, les point de passage critiques et les points de détention possibles.

Dans cette optique, il faut que la description soit réalisée de manière réaliste en fonction de l'architecture du système ainsi que des capacités du pirate.

Figure 23: digramme détaillé des attaques-scénarios opérationnels.



Source : préparée par nous même à travers les document fournis par la DGI

6.4.6. Évaluation de la vraisemblance des scénarios

Après avoir défini les scénarios, il faut ensuite les juger d'après leur vraisemblance, c'est-à-dire la probabilité de réalisation de ces scénarios dans l'environnement considéré. Il y a plusieurs aspects qui entrent en jeu pour juger un scénario, tels que sa complexité, l'importance des ressources qu'il demande et s'il existe des faiblesses pouvant être exploitées par le pirate informatique. Un scénario simple qui utilise des méthodes habituelles est jugé plus vraisemblable qu'un scénario compliqué.

Tableau 14:détaillé Évaluation de la vraisemblance des scénarios opérationnels

ID	Scénario opérationnel	Complexité de l'attaque	Ressources nécessaires	Existence de vulnérabilités	Vraisemblance
SO1	Compromission de comptes via phishing	Faible	Faibles	Élevée (facteur humain exploitable)	Élevée
SO2	Attaque DDoS sur l'infrastructure	Moyenne	Élevées	Moyenne (dépend des protections en place)	Moyenne
SO3	Abus de privilèges internes	Moyenne	Moyennes	Élevée (droits internes exploitables)	Élevée
SO4	Injection de requêtes malveillantes	Moyenne	Faibles	Moyenne (selon sécurisation applicative)	Moyenne
SO5	Exploitation d'une faille d'authentification	Élevée	Moyennes	Faible à moyenne (selon robustesse du système)	Faible

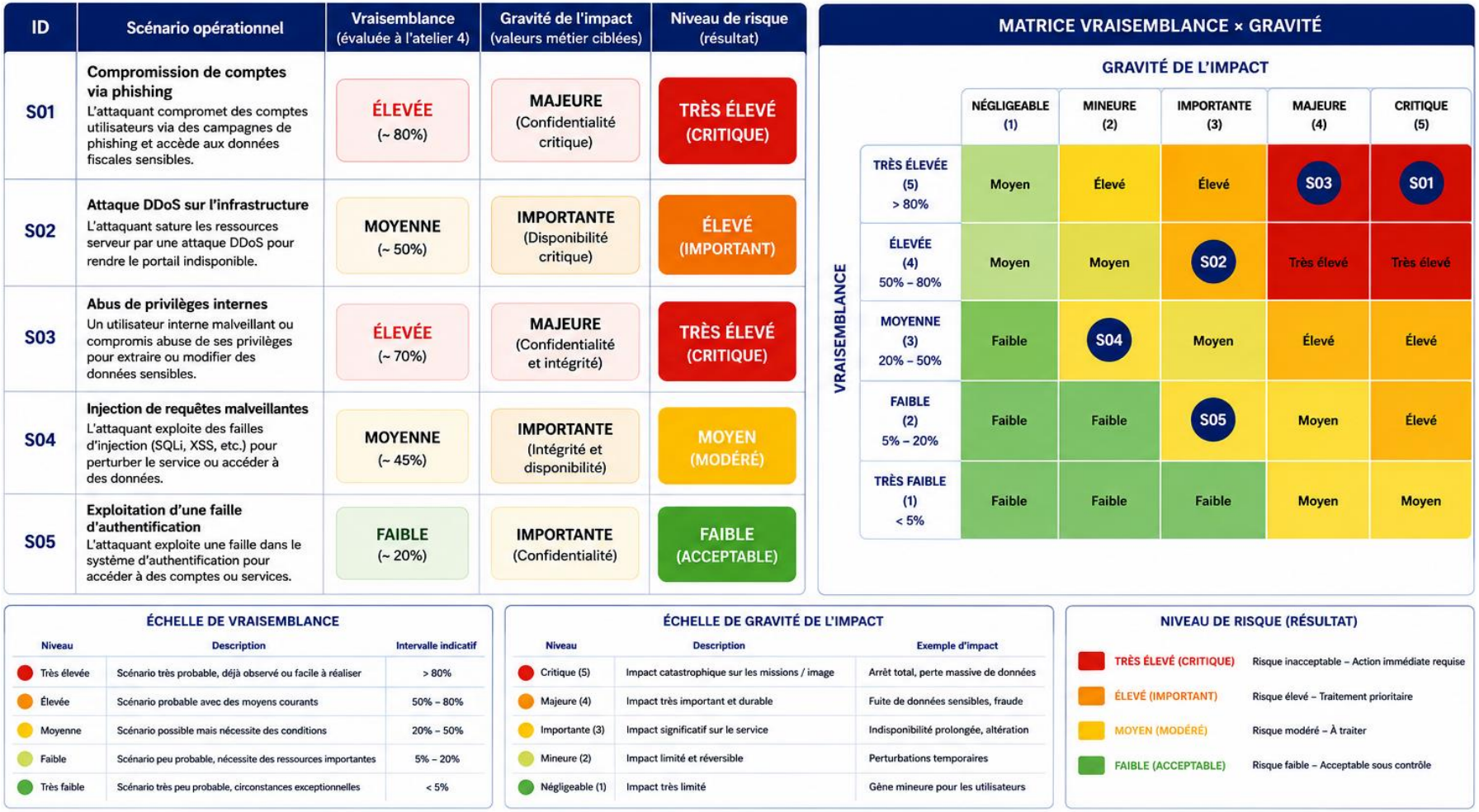
Source : préparée par nous même à travers les document fournis par la DGI

6.4.7. Détermination des niveaux de risque

Le niveau de risque est déterminé en combinant la gravité des impacts (identifiée dans les ateliers précédents) avec la vraisemblance des scénarios. Cette approche permet d'obtenir une vision globale du risque associé à chaque scénario opérationnel.

Les scénarios présentant à la fois une forte gravité et une forte vraisemblance sont considérés comme prioritaires et nécessitent des mesures de sécurité renforcées. À l'inverse, les scénarios moins probables ou ayant un impact limité peuvent être traités de manière secondaire.

Figure 24:détaillé Évaluation de la vraisemblance des scénarios opérationnels.



ID	Scénario opérationnel	Vraisemblance (évaluée à l'atelier 4)	Gravité de l'impact (valeurs métier ciblées)	Niveau de risque (résultat)
S01	**Compromission de comptes via phishing** L'attaquant compromet des comptes utilisateurs via des campagnes de phishing et accède aux données fiscales sensibles.	ÉLEVÉE (~ 80%)	MAJEURE (Confidentialité critique)	TRÈS ÉLEVÉ (CRITIQUE)
S02	**Attaque DDoS sur l'infrastructure** L'attaquant sature les ressources serveur par une attaque DDoS pour rendre le portail indisponible.	MOYENNE (~ 50%)	IMPORTANTE (Disponibilité critique)	ÉLEVÉ (IMPORTANT)
S03	**Abus de privilèges internes** Un utilisateur interne malveillant ou compromis abuse de ses privilèges pour extraire ou modifier des données sensibles.	ÉLEVÉE (~ 70%)	MAJEURE (Confidentialité et intégrité)	TRÈS ÉLEVÉ (CRITIQUE)
S04	**Injection de requêtes malveillantes** L'attaquant exploite des failles d'injection (SQLi, XSS, etc.) pour perturber le service ou accéder à des données.	MOYENNE (~ 45%)	IMPORTANTE (Intégrité et disponibilité)	MOYEN (MODÉRÉ)
S05	**Exploitation d'une faille d'authentification** L'attaquant exploite une faille dans le système d'authentification pour accéder à des comptes ou services.	FAIBLE (~ 20%)	IMPORTANTE (Confidentialité)	FAIBLE (ACCEPTABLE)

ÉCHELLE DE VRAISEMBLANCE

Niveau	Description	Intervalle indicatif
Très élevée	Scénario très probable, déjà observé ou facile à réaliser	> 80%
Élevée	Scénario probable avec des moyens courants	50% – 80%
Moyenne	Scénario possible mais nécessite des conditions	20% – 50%
Faible	Scénario peu probable, nécessite des ressources importantes	5% – 20%
Très faible	Scénario très peu probable, circonstances exceptionnelles	< 5%

ÉCHELLE DE GRAVITÉ DE L'IMPACT

Niveau	Description	Exemple d'impact
Critique (5)	Impact catastrophique sur les missions / image	Arrêt total, perte massive de données
Majeure (4)	Impact très important et durable	Fuite de données sensibles, fraude
Importante (3)	Impact significatif sur le service	Indisponibilité prolongée, altération
Mineure (2)	Impact limité et réversible	Perturbations temporaires
Négligeable (1)	Impact très limité	Gêne mineure pour les utilisateurs

NIVEAU DE RISQUE (RÉSULTAT)

TRÈS ÉLEVÉ (CRITIQUE)	Risque inacceptable – Action immédiate requise
ÉLEVÉ (IMPORTANT)	Risque élevé – Traitement prioritaire
MOYEN (MODÉRÉ)	Risque modéré – À traiter
FAIBLE (ACCEPTABLE)	Risque faible – Acceptable sous contrôle

Source : préparée par nous même à travers les document fournis par la DGI

6.4.8. Détermination des niveaux de risque

Synthèse de tous les scénarios examinés afin d'avoir une vue d'ensemble claire et structurelle des différents risques qui pèsent sur le système.

Il permet d'aider à prendre les bonnes décisions en se concentrant sur les scénarios les plus importants.

Le contenu de cette synthèse inclut tous les aspects des scénarios, en particulier leur source, leur objectif, leur probabilité et leur risque.

Tableau 15: niveaux de risque.

ID	Scénario opérationnel	Vraisemblance	Gravité de l'impact	Niveau de risque	Priorité de traitement
SO1	Compromission de comptes via phishing	Élevée	Critique (confidentialité)	Très élevé	Prioritaire
SO2	Attaque DDoS sur l'infrastructure	Moyenne	Importante (disponibilité)	Élevé	Élevée
SO3	Abus de privilèges internes	Élevée	Critique (confidentialité et intégrité)	Très élevé	Élevée
SO4	Injection de requêtes malveillantes	Moyenne	Importante (intégrité et disponibilité)	Moyen	Modérée
SO5	Exploitation d'une faille d'authentification	Faible	Importante (confidentialité)	Faible	Faible

Source : préparée par nous même à travers les document fournis par la DGI

6.4.9. Conclusion du 4eme atelier

Dans atelier 4 nous ont fourni une meilleure description des scénarios d'attaque, en mettant en évidence la manière précise dont elles peuvent être mises en œuvre sur la plateforme Jibaya'tic.

La caractérisation de la probabilité et la classification des niveaux de risque ont permis la hiérarchisation des menaces à partir des scénarios les plus dangereux.

Cette étape est cruciale car elle prépare les ateliers suivants, qui permettront de mettre en place les solutions adéquates pour limiter ces menaces.

Atelier 05 : traitement de risque

6.5. Objectif de l'atelier

La mission de ce travail est de déterminer les stratégies de sécurité pouvant faire face aux menaces évaluées dans les ateliers précédents. Cette activité sert à prendre en compte les actions à effectuer afin de préserver le portail Jibaya'tic des différents scénarii de menace qui lui sont attribués Il s'agit par conséquent d'une procédure consistant à trouver des actions techniques, opérationnelles ou organisationnelles visant à réduire la probabilité de réalisation

D'un scénario de menace ou à minimiser son impact sur les valeurs métier de la solution.

Ce travail nous permet aussi de définir une stratégie générale de réduction des risques prenant en compte les contraintes de la solution.

6.5.1. Priorisation des risques

Après l'identification des risques potentiels liés à la sécurité du système d'information du portail fiscal Jibaya'ti*c*, nous avons procédé à leur évaluation selon la méthode EBIOS Risk Manager. Cette évaluation repose sur la combinaison de deux critères fondamentaux : la **vraisemblance** du scénario d'attaque et la **gravité** de son impact sur les valeurs métier du portail. Le niveau de risque est calculé selon la formule suivante :

Niveau de risque = Vraisemblance × Gravité

Chaque critère est noté sur une échelle de 1 à 4 :

Tableau 16: Tableau de cotation des niveaux de vraisemblance et de gravité d'impact.

Niveau	Vraisemblance	Gravité de l'impact
1	Minime	Négligeable (G1)
2	Significative	Limitée (G2)
3	Forte	Grave (G3)
4	Maximale	Critique (G4)

Source : ((ANSSI), September 2024.)

Les intervalles de criticité ont été établis comme suit :

Tableau 17: Tableau des intervalles de criticité et des niveaux de risque associés.

Intervalle	**Niveau de risque**	**Justification**
1 à 4	Risque acceptable	Combinaison de critères de (1×1) à (2×2)
5 à 9	Risque élevé	Combinaison de critères de (2×2) à (3×3)
10 à 16	Risque très élevé (prioritaire)	Combinaison de critères de (3×3) à (4×4)

Source : préparée par nous même à travers les document fournis par la DGI

6.5.2. Évaluation et acceptation des risques

Sur la base de cette grille, nous avons évalué les **cinq scénarios opérationnels** identifiés lors des ateliers EBIOS RM et déterminé leur niveau d'acceptabilité. Le seuil d'acceptation du risque a été défini en concertation avec les responsables du bureau de la sous-direction de la gouvernance et de la sécurité des systèmes d'information fiscale (SDGSIF) de la DGI.

Tableau 18: Tableau d'évaluation des scénarios opérationnels selon le niveau de risque et la priorité de traitement.

	Scénario opérationnel	**Vraisemblance**	**Gravité**	**Niveau de risque**	**Priorité**
SO1	Compromission de comptes via phishing	Élevée (3)	Critique G4 (4)	**12 — Très élevé**	Prioritaire

SO2	Attaque DDoS sur l'infrastructure	Moyenne (2)	Grave G3 (3)	**6 — Élevé**	Élevée
SO3	Abus de privilèges internes	Élevée (3)	Critique G4 (4)	**12 — Très élevé**	Élevée
SO4	Injection de requêtes malveillantes	Moyenne (2)	Grave G3 (3)	**6 — Moyen**	Modérée
SO5	Exploitation d'une faille d'authentification	Faible (1)	Grave G3 (3)	**3 — Faible**	Faible

Source : préparée par nous même à travers les document fournis par la DGI

6.5.3. Tableau récapitulatif de l'acceptabilité

Tableau 19: Tableau récapitulatif de l'acceptabilité.

Niveau de risque	Acceptabilité	Nombre de scénarios (avant traitement)
1 à 4	Risque acceptable	**1** (SO5)
5 à 9	Risque élevé — non acceptable	**2** (SO2, SO4)
10 à 16	Risque très élevé — non acceptable, traitement urgent	**2** (SO1, SO3)

Source : préparée par nous même à travers les document fournis par la DGI

L'acceptation du risque n'implique pas son ignorance, mais la reconnaissance formelle que le niveau résiduel est conforme au seuil de tolérance défini par la DGI dans sa politique de sécurité. Tout risque dont le niveau excède ce seuil est orienté vers un plan de traitement structuré.

6.5.4. Traitement des risques

Dans le cadre de cet atelier 5, nous avons élaboré des plans de traitement pour chaque scénario dont le niveau de criticité dépassait le seuil d'acceptabilité. Les mesures proposées s'appuient sur les résultats des entretiens conduits auprès des membres du bureau de la SDGSIF et sur les

recommandations du référentiel EBIOS RM, en tenant compte des contraintes organisationnelles, techniques et réglementaires (code général des impôts, loi n° 18-07 sur la protection des données personnelles, loi n° 25-11).

Quatre types de traitement ont été appliqués :

- **Réduction :** mise en œuvre de mesures de sécurité diminuant la vraisemblance ou l'impact.
- **Transfert :** délégation partielle du risque à un tiers (hébergeur, prestataire sécurité).
- **Évitement :** suppression de l'activité ou du composant à l'origine du risque.
- **Acceptation :** maintien du risque résiduel dans les limites du seuil toléré, avec documentation formelle.

➢ **Risque SO1 — Compromission de comptes utilisateurs via phishing (Niveau : 12, Prioritaire)**

Tableau 20: Mesures de traitement du risque de compromission des comptes utilisateurs via phishing (SO1).

Élément	**Détail**
Mode de défaillance	Un cybercriminel compromet des comptes utilisateurs via des techniques de phishing pours accéder aux données fiscales sensibles
Valeur métier ciblée	- Données fiscales - Comptes utilisateurs
Niveau de risque brut	12 (Vraisemblance Élevée × Gravité Critique G4)
Type de traitement	Réduction
Mesures retenues (PA1)	- Déploiement de l'authentification multi-facteurs (MFA) - Sensibilisation des utilisateurs au phishing et à l'ingénierie sociale - Renforcement de la politique de mots de passe

	- Journalisation des tentatives d'accès
Responsables	- Équipe sécurité / Équipe IT: configuration et supervision - Agents DGI: respect de la charte de sécurité
Échéance	- Court terme: activation du MFA et journalisation - 30 jours: sessions de sensibilisation - 90 jours: audit des accès
Suivi	Revue mensuelle par la SDGSIF; audit semestriel des comptes

Source : préparée par nous même à travers les document fournis par la DGI.

- **Risque SO3 — Abus de privilèges internes (Niveau : 12, Élevée)**

Tableau 21: Mesures de traitement du risque de Abus de privilèges internes (SO3).

Élément	**Détail**
Mode de défaillance	Un employé disposant d'un accès privilégié exploite les systèmes internes SAP pour consulter ou extraire des données fiscales sensibles sans autorisation
Valeur métier ciblée	- Données fiscales - Intégrité et confidentialité
Niveau de risque brut	12 (Vraisemblance Élevée × Gravité Critique G4)
Type de traitement	Réduction
Mesures retenues (PA3)	- Renforcement de la gestion des habilitations et des privilèges (IAM) - Application du principe du moindre privilège - suppression du partage de comptes administrateurs

	- Mise en place d'un système avancé de journalisation (PA4)
Responsables	Administration système: gestion des droits d'accès - Équipe sécurité: surveillance et audit
Échéance	- Moyen terme: revue complète des habilitations SAP - 60 jours: Déploiement du système de journalisation
Suivi	Audit trimestriel des droits d'accès; revue semestrielle des comptes privilégiés

Source : préparée par nous même à travers les document fournis par la DGI

- **Risque SO2 — Attaque DDoS sur l'infrastructure (Niveau : 6, Élevée)**

Tableau 22: Mesures de traitement de l'Attaque DDoS sur l'infrastructure (SO2).

Élément	**Détail**
Mode de défaillance	Un attaquant cible l'infrastructure d'hébergement via une attaque DDoS pour rendre le portail Jibaya'tic indisponible lors des périodes de déclaration obligatoire
Valeur métier ciblée	- Continuité de service - Disponibilité du portail
Niveau de risque brut	6 (Vraisemblance Moyenne × Gravité G3)
Type de traitement	Réduction
Mesures retenues (PA2)	- Déploiement d'une solution de protection anti-DDoS - Redondance des infrastructures - Mécanismes de haute disponibilité

	- Plan de continuité d'activité (PCA)
Responsables	- Hébergeur / Infrastructure: mise en place des protections - DSI: validation du PCA
Échéance	- Court terme: activation des protections anti-DDoS - 60 jours: tests de basculement
Suivi	Simulation semestrielle; revue annuelle du PCA

Source : préparée par nous même à travers les document fournis par la DGI

6.5.5. Suivi et contrôle

Dans le cadre de la simulation de mise en œuvre de la méthode EBIOS Risk Manager sur le portail fiscal **Jibaya'tic**, les cinq ateliers ont permis d'identifier et d'évaluer **5 scénarios opérationnels prioritaires**, évalués selon leur niveau de vraisemblance et de gravité d'impact. Les résultats initiaux avant traitement révèlent la répartition suivante :

Tableau 23: Tableau d'évolution des niveaux d'acceptabilité des risques avant et après traitement.

Niveau d'acceptabilité	Nombre avant traitement	Nombre après traitement
Risque acceptable (1–4)	**1** (SO5)	**3** (SO2, SO4, SO5)
Risque élevé (5–9)	**2** (SO2, SO4)	**2** (SO1, SO3 — risque résiduel contrôlé)
Risque très élevé/prioritaire (10–16)	**2** (SO1, SO3)	**0**

Source : préparée par nous même à travers les document fournis par la DGI

Suite à la définition et à l'application du plan d'action de sécurité (PA1 à PA4), une réévaluation de chaque scénario a été réalisée en concertation avec les responsables de la SDGSIF. Cette réévaluation montre que :

- Les **2 risques très élevés** (SO1 et SO3), dont le niveau initial était de 12, ont été ramenés à un niveau résiduel contrôlé grâce au déploiement du MFA, à la gestion stricte des habilitations IAM et à la journalisation avancée.
- Les **2 risques élevés** (SO2 et SO4) ont été réduits à un niveau acceptable grâce aux protections anti-DDoS et au renforcement de la sécurisation applicative.
- Le **risque faible** SO5 demeure acceptable avec les mesures existantes, sous réserve d'une surveillance continue.

Ces résultats démontrent la faisabilité et la pertinence de la méthode EBIOS Risk Manager appliquée au contexte d'une administration fiscale numérique complexe. Ils confirment également, comme le soulignent les entretiens réalisés auprès des membres du bureau de la SDGSIF, que le facteur humain constitue le premier vecteur de vulnérabilité — la compromission via phishing (SO1) et l'abus de privilèges internes (SO3) étant les scénarios les plus critiques, avec un impact de gravité G4 sur les données fiscales des contribuables.

Ces résultats soulignent enfin la nécessité d'inscrire la gestion des risques dans une démarche continue et structurée, intégrée à la gouvernance globale du système d'information de la DGI, et non comme une intervention ponctuelle. La formalisation d'une politique de gestion des risques SI, s'appuyant sur EBIOS RM et l'outil CISO Assistant, constitue à cet égard la première recommandation pratique issue de cette étude.

6.5.6. Évaluation des mesures de sécurité

L'atelier 5 a permis de définir les mesures de sécurité nécessaires pour réduire les risques identifiés tout au long de l'analyse EBIOS RM appliquée au portail Jibaya’tic.

Les décisions relatives au traitement des risques doivent être validées par les responsables concernés afin de garantir leur cohérence avec les objectifs stratégiques et opérationnels du système. Cette validation permet de confirmer que les mesures retenues répondent correctement aux risques identifiés et que les ressources nécessaires à leur mise en œuvre peuvent être mobilisées. Elle constitue également une étape importante dans la gouvernance globale de la sécurité du système d'information.

Les mesures retenues ont été évaluées puis organisées dans un plan d'action structuré afin d'assurer une amélioration progressive du niveau de sécurité du système. L'identification des risques résiduels a également permis de conserver une vision réaliste des menaces pouvant subsister après traitement.

Cette dernière étape clôture l'analyse EBIOS RM du portail Jibaya’tic en fournissant une approche globale et cohérente de gestion des risques liés à la cybersécurité du système.

Section 02 : Discussion des résultats

La présente section vise à confronter les résultats obtenus lors de notre terrain d'investigation à la Direction Générale des Impôts (DGI) avec les apports de la revue de littérature et les enseignements théoriques et méthodologiques mobilisés tout au long de ce travail. Les données collectées combinent des entretiens semi-directifs menés auprès du bureau de la sous-direction de la gouvernance et de la sécurité des systèmes d'information fiscale, une analyse documentaire approfondie, ainsi qu'une application pratique de la méthode EBIOS Risk Manager sur le portail Jibaya’tic. Cette triangulation permet d'apprécier la cohérence interne des résultats et d'en dégager des implications à la fois pratiques et théoriques.

7. Interprétation des résultats

Les résultats issus des entretiens révèlent une réalité organisationnelle marquée par l'absence d'une politique formalisée et documentée de gestion des risques liés à la sécurité des systèmes d'information au sein de la DGI. Les trois répondants convergent sur ce constat, soulignant que les dispositifs existants se limitent à une charte de sécurité générale, sans déclinaison opérationnelle suffisante. Ce constat rejoint directement les lacunes identifiées dans la revue de littérature, notamment par (Adel & DAHIA , 2022), qui relevait que le système fiscal algérien rencontre des difficultés dans la mise en place d'un cadre unifié de gestion des risques menaçant la sécurité de son système d'information.

Par ailleurs, les résultats confirment les observations de (Sabr & ZERDOUDI , 2022)qui soulignaient la nécessité d'adopter sérieusement un système de management de la sécurité de l'information (SMSI) conforme aux normes internationales dans les établissements algériens. En effet, bien que la DGI dispose de mesures techniques solides — notamment les solutions SAN DORADO et le site miroir auprès d'Algérie Télécom — ces mesures restent circonscrites à la dimension technique sans s'inscrire dans une démarche globale et structurée de gestion des risques.

De surcroît, la forte cohérence lexicale observée entre les trois entretiens (coefficients de corrélation entre 0,947 et 0,953) témoigne d'une vision partagée et homogène des enjeux sécuritaires au sein de l'équipe interrogée. Cette convergence de discours renforce la fiabilité des données collectées et confirme que les difficultés identifiées ne sont pas le reflet d'une

perception individuelle isolée, mais bien d'une réalité organisationnelle consensuelle, au sens des travaux de (Flick, 2018) sur la triangulation des données qualitatives.

8. Discussion critique des résultats

Si les résultats obtenus confirment globalement les cadres théoriques mobilisés, il convient néanmoins d'en soumettre certains aspects à une analyse critique. Le premier point de tension concerne la nature du facteur humain identifié comme principal obstacle à l'efficacité de la gestion des risques. Les répondants évoquent le manque de coordination, l'insuffisance de communication interne et la faiblesse du partage d'informations entre les parties prenantes. Ces observations corroborent les travaux de (KHEIRA, 2012)qui insistait sur le rôle de l'usage incorrect des TIC comme source de risques organisationnels, et de (Mohamed & Ahmed Gaid , 2017) , qui plaçait le facteur humain au cœur des risques liés aux systèmes d'information.

Le second point critique tient aux perspectives d'évolution exprimées par les participants. L'évocation du décret présidentiel n° 07-26 du 5 janvier 2026 relatif à la structure de sécurité des systèmes d'information, ainsi que la création envisagée d'une direction dédiée à la sécurité SI au sein de la DGI, témoignent d'une volonté institutionnelle réelle. Toutefois, comme le soulignait (RABII, 2023)dans sa thèse Atla Sec, ce n'est pas le manque de standards de sécurité qui constitue le problème fondamental, mais bien la capacité à les mettre en œuvre dans un système complexe. La DGI, en tant que système complexe intégrant plusieurs directions régionales, des plateformes numériques interconnectées et des bases de données fiscales sensibles, illustre précisément cette problématique.

Enfin, la classification des incidents en deux catégories — fonctionnels et de sécurité — telle que présentée par les répondants, s'aligne avec la typologie des risques proposée dans la littérature (felidj, miguel, & virginie , 2021) , distinguant les risques physiques, logiques et humains. Cependant, nos résultats montrent que la DGI n'a pas encore développé une cartographie systématique de ces risques, ce qui constitue une lacune importante au regard des exigences de la norme ISO/IEC 27005.

9. Comparaison avec la littérature et les pratiques internationales

La comparaison des résultats obtenus avec les pratiques documentées dans la littérature met en évidence plusieurs convergences significatives. Premièrement, l'absence de politique formalisée de gestion des risques SI à la DGI confirme le constat formulé par (Ministère de la Poste, des Télécommunications, 2020), selon lequel la sécurité des systèmes d'information du secteur public algérien nécessite un cadre national unique fondé sur l'identification, l'évaluation

et le traitement des risques. Deuxièmement, le faible taux d'application des normes de sécurité dans les institutions publiques algériennes — relevé à 67,14 % en moyenne par (MAHRRAR & KERZABI, 2021)— trouve un écho direct dans les insuffisances identifiées lors de nos entretiens.

Sur le plan méthodologique, l'application de la méthode EBIOS Risk Manager au portail Jibaya'tic permet de démontrer la pertinence de cette approche dans le contexte institutionnel algérien. Conformément à l'analyse comparative réalisée, EBIOS RM présente plusieurs avantages déterminants par rapport aux méthodes alternatives MEHARI et OCTAVE : son ancrage dans le contexte institutionnel public francophone, sa conformité aux normes ISO 27001, ISO 27005 et ISO 31000, sa gratuité et son adoption par plusieurs administrations fiscales francophones, notamment en Belgique, en Tunisie et au Québec. Ces arguments rejoignent les recommandations formulées par ((ANSSI), September 2024.),qui positionne EBIOS RM comme le référentiel de prédilection pour l'appréciation et le traitement des risques numériques dans les organisations publiques.

L'application des cinq ateliers de la méthode EBIOS RM au portail Jibaya'tic a permis d'identifier cinq scénarios opérationnels prioritaires. Parmi ceux-ci, la compromission de comptes utilisateurs via phishing (SO1) et l'abus de privilèges internes (SO3) ont été évalués comme les risques les plus critiques, avec un niveau de vraisemblance élevé combiné à un impact de gravité G4 sur les données fiscales. Ces résultats corroborent les observations de (felidj, miguel, & virginie , 2021)sur la prédominance des risques humains et logiques dans les systèmes d'information, et confirment que le facteur humain demeure le premier vecteur de vulnérabilité, conformément aux déclarations des répondants lors des entretiens.

Par ailleurs, l'analyse des écarts conduite dans l'atelier 1 d'EBIOS RM a mis en lumière des défaillances spécifiques, notamment le partage de comptes administrateurs et la gestion insuffisante des habilitations dans l'environnement SAP. Ces constats rejoignent les observations de (Alexei, 2021)sur la nécessité de garantir une conformité adéquate aux standards internationaux pour établir la confiance dans la sécurité des systèmes d'information publics.

10. Implications pratiques

Les résultats de cette recherche comportent des implications pratiques, théoriques et institutionnelles qui méritent d'être explicitées.

Sur le plan pratique, les résultats suggèrent que la DGI devrait s'engager dans une démarche structurée en plusieurs axes complémentaires. En premier lieu, la formalisation d'une politique de gestion des risques SI, s'appuyant sur la méthode EBIOS RM et l'outil CISO Assistant, permettrait de combler le vide institutionnel identifié. CISO Assistant, solution open source développée par la société française intuitem, se distingue comme l'outil le mieux adapté aux exigences de la DGI en raison de son support natif d'EBIOS RM, de sa souveraineté totale des données via déploiement local, et de sa conformité aux normes ANSSI — des caractéristiques particulièrement adaptées au contexte de souveraineté numérique algérienne.

En deuxième lieu, il conviendrait de renforcer la sensibilisation et la formation des utilisateurs aux risques cyber, en particulier au phishing et à l'ingénierie sociale, qui constituent les vecteurs d'attaque les plus vraisemblables identifiés dans les scénarios opérationnels. En troisième lieu, la mise en place d'une gestion stricte des identités et des accès (IAM), appliquant le principe du moindre privilège, permettrait de réduire significativement le risque d'abus de privilèges internes.

Sur le plan théorique, cette recherche contribue à combler une lacune identifiée dans la revue de littérature : l'absence d'études appliquées à la gestion des risques SI dans les administrations fiscales publiques algériennes. Elle démontre la faisabilité et la pertinence d'une application d'EBIOS RM à un système d'information fiscal complexe, offrant ainsi un cadre de référence reproductible pour d'autres institutions similaires.

Sur le plan institutionnel, nos résultats soulignent l'importance des évolutions réglementaires récentes — notamment le décret présidentiel n° 07-26 et l'instruction du ministère des Finances relative à la création de directions dédiées à la sécurité SI — comme leviers essentiels pour accompagner la maturité organisationnelle en matière de cybersécurité au sein de la DGI.

Pour de futures recherches, il serait utile d'explorer l'impact des mécanismes de gouvernance SI sur l'efficacité du processus de gestion des risques dans les administrations fiscales, ou encore d'évaluer le degré d'adoption des normes ISO 27001 et ISO 27005 dans l'ensemble des directions relevant du ministère des Finances algérien.

À partir de cette étude, il apparaît clairement que la gestion des risques liés à la sécurité des systèmes d'information connaît une évolution notable et s'inscrit dans une perspective prometteuse. Malgré l'absence d'une politique formalisée et clairement définie, les différents efforts déployés au sein de la Direction Générale des Impôts constituent un indicateur positif de son développement dans les années à venir. L'adoption de la méthode EBIOS représente ainsi une première étape vers une amélioration significative de la gestion des risques au sein de la Direction Générale des Impôts.

CONCLUSION GÉNÉRALE

Dans un contexte de développement rapide du domaine numérique et de dépendance croissante aux systèmes d'information dans la gestion des institutions publiques, les questions relatives à la sécurité des systèmes d'information et à la gestion des risques associés sont devenues des priorités stratégiques incontournables. En effet, les administrations font aujourd'hui face à des défis de plus en plus importants liés aux cyberattaques, aux faiblesses du contrôle des accès, ainsi qu'aux risques humains et organisationnels susceptibles d'affecter directement la confidentialité, l'intégrité des données et la continuité des services.

Dans ce cadre, cette recherche s'inscrit dans l'étude de la gestion des risques liés à la sécurité des systèmes d'information au niveau de la Direction Générale des Impôts, avec pour objectif d'analyser la situation actuelle de la sécurité informatique au sein de cette institution, d'identifier les principaux risques menaçant ses systèmes, notamment ceux liés aux plateformes fiscales, et de proposer un cadre méthodologique de gestion de ces risques basé sur la méthode EBIOS Risk Manager. Cette étude a adopté une approche méthodologique combinant une analyse qualitative à travers des entretiens avec les acteurs de la gouvernance et de la sécurité des systèmes d'information, et une analyse appliquée via une étude de cas du portail Jibaya'tic, ce qui a permis une compréhension approfondie de la réalité sécuritaire au sein de la Direction Générale des Impôts.

Dans cette perspective, cette conclusion vise à présenter les principaux résultats obtenus, à mettre en évidence les contributions scientifiques et pratiques de la recherche, ainsi qu'à discuter de ses limites, tout en ouvrant des perspectives susceptibles de développer les pratiques de gestion des risques des systèmes d'information et de renforcer la maturité sécuritaire au sein des institutions publiques**.**

- **Résultats de la recherche**

Dans cette continuité, la pertinence des résultats issus des entretiens menés auprès des membres du bureau de la sous-direction de la gouvernance et de la sécurité des systèmes d'information fiscale a permis de dégager une vision globale et cohérente de la situation actuelle. Les trois répondants convergent sur le constat de l'absence d'une politique formalisée et documentée de gestion des risques SI au sein de la DGI, les dispositifs existants se limitant à une charte de sécurité générale sans déclinaison opérationnelle suffisante La conclusion la plus évidente qui ressort est que, bien que la DGI dispose de mesures techniques solides notamment les solutions SAN DORADO et le site miroir auprès d'Algérie

Télécom , ces mesures restent circonscrites à la dimension technique sans s'inscrire dans une démarche globale et structurée de gestion des risques. Par ailleurs, le facteur humain apparaît comme le principal vecteur de vulnérabilité, à travers le manque de coordination entre les parties prenantes, l'insuffisance de communication interne et la faiblesse du partage d'informations. L'application des cinq ateliers de la méthode EBIOS Risk Manager au portail Jibaya'tic a permis d'identifier cinq scénarios opérationnels prioritaires, parmi lesquels la compromission de comptes utilisateurs via des attaques de phishing et l'abus de privilèges internes se révèlent les plus critiques, avec un niveau de vraisemblance élevé combiné à un impact de gravité G4 sur les données fiscales. Ces résultats confirment la prédominance des risques humains et logiques dans les systèmes d'information fiscaux. Parallèlement, les implications de l'étude intègrent plusieurs axes d'action prioritaires. En premier lieu, la formalisation d'une politique de gestion des risques SI s'appuyant sur la méthode EBIOS RM et l'outil CISO Assistant, solution open source offrant un support natif d'EBIOS RM, une souveraineté totale des données et une parfaite adéquation au cadre de souveraineté numérique algérienne. En deuxième lieu, le renforcement de la sensibilisation et de la formation des utilisateurs aux risques cyber, en particulier au phishing et à l'ingénierie sociale. En troisième lieu, la mise en place d'une gestion stricte des identités et des accès appliquant le principe du moindre privilège, afin de réduire significativement le risque d'abus de privilèges internes. Ces stratégies d'exécution permettent de rationaliser la posture sécuritaire de la DGI, en assurant la confidentialité, l'intégrité et la disponibilité des données fiscales sensibles, et partant, la confiance des contribuables envers l'institution.

- **Limites de la recherche**

En dépit de la pertinence et des implications de notre étude, plusieurs limites doivent être appréciées, notamment :

- La récence et le manque de littérature académique spécifiquement centrée sur la gestion des risques SI dans les administrations fiscales publiques algériennes, ce qui a rendu la comparaison avec des travaux similaires partiellement difficile.
- Le manque d'accès et d'exhaustivité des données probantes internes à la DGI, en raison des contraintes de confidentialité inhérentes aux institutions publiques fiscales.
- La taille réduite de l'échantillon des entretiens, limitée à trois répondants au sein du bureau de la sous-direction de la gouvernance et de la sécurité des systèmes

d'information fiscale, ce qui restreint la généralisation des résultats à l'ensemble de la direction.

- Les biais de réponses liés aux déclarations des participants, susceptibles de ne pas refléter intégralement la réalité des pratiques organisationnelles en matière de gestion des risques
- Le manque de collaboration partielle de certaines parties prenantes internes à la DGI, qui a limité l'accès à des informations plus détaillées nécessaires à la concrétisation de l'étude.

➢ **Les recommandations**

- Élaboration et adoption d'une politique formelle de gestion des risques liés à la sécurité des systèmes d'information, conforme aux normes internationales, avec des objectifs mesurables et l'utilisation d'outils appropriés.
- Mise en œuvre de programmes continus de sensibilisation et de formation du personnel aux risques cybernétiques et aux meilleures pratiques de sécurité.
- Application du principe du moindre privilège et adoption de l'authentification multi facteur afin de réduire les risques liés à l'abus de privilèges.
- Déploiement de systèmes avancés de surveillance et d'analyse permettant de détecter rapidement les menaces et d'améliorer la réponse aux incidents.
- Mise en place de plans clairs et éprouvés pour la gestion des incidents et la continuité des activités dans diverses situations.
- Renforcement de la gouvernance de la sécurité par la désignation d'un responsable spécialisé et la mise à disposition des ressources nécessaires à la mise en œuvre de la stratégie de cybersécurité.

➢ **Prolongements et voies futures de la recherche**

Cette recherche a mis en lumière l'intérêt encore insuffisamment exploré de la gestion des risques SI dans les administrations fiscales publiques algériennes, ouvrant ainsi plusieurs perspectives de prolongement. Des investigations plus approfondies pourraient inclure l'évaluation du degré de conformité aux normes ISO 27001 et ISO 27005 dans l'ensemble des directions relevant du ministère des Finances algérien, ainsi que la mesure de l'impact des nouvelles structures dédiées à la sécurité SI telles que prévues par le décret présidentiel n° 07-26 du 5 janvier 2026 sur la maturité organisationnelle de la DGI en matière de cybersécurité. En outre, une perspective d'étude longitudinale permettrait d'évaluer l'évolution du niveau de maturité de la gestion des risques SI au fil du temps, offrant ainsi

aux chercheurs la possibilité d'explorer l'impact réel des programmes de renforcement des capacités et des politiques de sécurité mises en œuvre dans le cadre du modèle proposé.

REFERENCES BIBLIOGRAPHIQUES

1. Adel, B., & Dahia, A. (2022, 31 octobre). *Le contrôle interne : dispositif permanent et indispensable pour la maîtrise des risques liés aux systèmes d'information*.
2. Alexei, A. (2021, 2 janvier). *Ensuring Information Security in Public Organizations in the Republic of Moldova Through the ISO 27001 Standard*. *Journal of Social Sciences Moldova*. DOI : à compléter.
3. ANSSI. (2024, septembre). *EBIOS Risk Manager : La sécurité des systèmes d'information*. Paris : ANSSI.
4. Baikady, I., & Khan, A. (2022). *Principles of Social Research Methodology*.
5. Bowen, G. A. (2009). *Document Analysis as a Qualitative Research Method*.
6. CLUSIF. (2022). *MEHARI – Standard*. URL : https://clusif.fr/mehari/
7. CLUSIF. (2025, septembre). *Guide de la cybersécurité des systèmes industriels*. France : Club de la Sécurité de l'Information Français. URL : https://clusif.fr/
8. Creswell, J. W. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*.
9. David, A. (2000). *La recherche-intervention, cadre général pour la recherche en management*. Dans A. David, A. Hatchuel, & R. Laufer (dir.), *Les nouvelles fondations des sciences de gestion*. Paris : Vuibert.
10. Direction Générale des Impôts. *About Us / Données générales*. URL : https://www.mf.gov.dz/index.php/fr/services-2/impots/27-la-direction-generale-des-impots-ses-missions
11. Direction Générale des Impôts. *Présentation de la Direction Générale des Impôts*. URL : https://www.mfdgi.gov.dz/fr/a-propos/dgi
12. Felidj, C., Miguel, L., & Virginie, B. (2021). *Management des systèmes d'information*. Malakoff : Francis Lefebvre.
13. Flick, U. (2018). *The SAGE Handbook of Qualitative Data Collection*. London : SAGE Publications.
14. Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). *Methods of Data Collection in Qualitative Research*. *British Dental Journal*, 204, 291–295.
15. ISO. (2018). *ISO 31000 – Risk Management Guidelines*. URL : https://www.iso.org/standard/65694.html
16. Jugier. (2021). *6.1 Actions liées aux risques et opportunités*. Protectam. URL : https://www.protectam.fr/
17. Khaled, R., Ben Ammara, T., & Dhouar, M. (2018, 31 décembre). *Évaluation de la performance du système d'information électronique : étude comparative entre*

l'Office National de la Météorologie et l'entreprise HESS. *Revue des sciences économiques et des sciences de gestion*.

18. Kheira, A. (2012). *Les risques liés aux TIC dans l'entreprise : essai d'analyse à partir d'un échantillon d'entreprises algériennes*.
19. Laudon, K., & Laudon, J. (2017). *Management des systèmes d'information*. Paris : Pearson Education France.
20. Lupfer, A. (2010). *Gestion des risques en sécurité de l'information*. Paris : Eyrolles.
21. Mahrar, A., & Kerzabi, A. (2021, 31 décembre). *Le système d'information en Algérie : un saut compétitif pour les entreprises algériennes*.
22. Miles, M., & Huberman, A. (1991). *Analyse des données qualitatives*.
23. Ministère de la Poste et des Télécommunications. (2020). *Référentiel National de Sécurité de l'Information*.
24. Mohamed, A., & Ahmed Gaid, N. (2017). *Contribution de l'audit interne dans la gestion des risques liés aux systèmes d'information dans le cadre de la gouvernance des systèmes d'information : cas Evolutec International – Algérie*. *Biskra Journal of Industrial Economics*.
25. Pons, J.-C. (2022). *La norme ISO 27005*. Herblain : Epsilon.
26. Rabii, A. (2023, 4 juillet). *Une approche pour la maîtrise de la sécurité de l'information adaptée aux systèmes de systèmes*. Rabat, Maroc.
27. Sabr, M., & Zerdoudi, A. (2022, 1 juin). *L'évaluation du système de management de la sécurité de l'information (SMSI) aux normes internationales ISO 27001 : étude de cas de l'entreprise portuaire de Skikda – Algérie*. *Revue des sciences humaines et sociales*.
28. Solomon, P., & Cox, D. R. (2014). *Components of Variance*. Chapman & Hall/CRC.
29. Thiétart, R.-A. (2014). *Méthodes de recherche en management*.
30. Varinard, C. (2018). *Système d'information de gestion*. Paris : Éditions Ellipses.
31. Wittorski, R., & Daverne-Bailly, C. (2022). *Research Methodology in Education and Training : Postures*. Wiley.

ANNEXES

ANNEXE A :

GUIDE D'ENTRETIEN

Guide d'entretien

Bonjour, nous sommes étudiantes en Master 2 gouvernement électronique. Dans le cadre de notre mémoire de fin d'études, nous réalisons une étude Sur « gestion des risques liée à la sécurité des systèmes d'informations de la DGI ». Cet entretien a pour but d'évaluer la maturité de la gestion des risques liés à la sécurité du système d'information de la Direction

Vos réponses resteront confidentielles et seront utilisées uniquement à des fins Académiques.

1) Pouvez-vous nous présenter les missions et les fonctions de DSI ?
2) Quels sont les systèmes utilisés pour la gestion des activités fiscales et la responsabilité de la direction dans le développement de ces systèmes ?
3) Existe-t-il une politique pour la gestion des risques de sécurité si ?
4) Quels sont les incidents auxquels le système d'information de la direction fait face ?
5) Quelles sont les garanties de sécurité, sauvegarde et récupération des données fiscales dans le système d'information ?
6) Quels sont les défis et les contraintes qui limitent l'efficacité de la gestion des risques au sein de la direction ?
7) Quelles sont vos perspectives d'avenir concernant le développement de la sécurité du système d'information et l'amélioration de la gestion des risques au sein de la direction ?

ANNEXE B :

SHÉMA D'INTERCONNEXION DU RÉSEAU MPLS DE LA DGI ET DE SES STRUCTURES DÉCONECENTRÉES


DGI-MDF 01
LS DATA
+
INTERNET
DGE 01
LS DATA IP/MPLS
CDI 49
LS DATA IP/MPLS
CPI 105
LS DATA IP/MPLS
LS DATA IP/MPLS
DIW 43
LS DATA IP/MPLS
DRI 9
LS DATA IP/MPLS
SRV 03

ANNEXE C :

MATRICE D'ANALYSE THEMATIQUE

Les questions	A: entretien 01	B: entretien 02	C: Entretien 03
Pouvez-vous nous présenter les missions et les fonctions de DSI ?	D'une connaissance réglementaire des tâches claires, écrites et définies par des textes exécutifs précis comme assurer la synergie du système d'information avec la stratégie globale et les exigences des métiers de la direction générale des impôts et intégrer au sein du système d'information les dernières évolutions technologiques enregistrées en la matière pour les fonctions, la Direction générale est divisée En quatre sous-directions	La direction des systèmes d'information ses missions et son organisation récentes sont définies par le décret exécutif n°21-252 La DSI est chargée d'assurer la gestion opérationnelle des systèmes applicatifs, des infrastructures, du réseau et de leur sécurité ainsi que d'apporter assistance et supports aux utilisateurs et établir et de déployer la Politique de sécurité visant à assurer l'intégrité des données, la sécurité des accès aux applications et aux équipements et la	La DSI s'inscrit dans un cadre réglementaire précis défini par le décret exécutif N°21-252 Ses missions sont clairement établies par des textes législatifs, notamment la synchronisation du système d'information avec la stratégie générale de la Direction Générale des Impôts l'intégration continue des nouvelles technologies dans ce système le plan organisationnel
Quels sont les systèmes utilisés pour la gestion des activités fiscales et la responsabilité de la direction dans le développement de ces systèmes ?	Les systèmes de la Direction Générale des Impôts sont variés et reposent sur quatre services numériques principaux Jibaya'tic le terme Jibaya'tic est la prononciation de la transcription du mot « fiscalité » en arabe et « TIC » correspond aux technologies de l'information et de la communication, il offre les services de	La Direction Générale des Impôts dispose de plusieurs systèmes conçus de manière simple et numérique afin de faciliter leur utilisation et de promouvoir les services de paiement dans le domaine fiscal. Elle propose ainsi quatre services numériques principaux	Quatre plateformes principales Jibaya'tic, est la plateforme de déclaration fiscale en ligne. Elle permet aux contribuables de soumettre leurs déclarations à distance dans un environnement ergonomique et sécurisé Tabioucom, offre la possibilité d'effectuer le paiement des timbres

	déclaration d'impôts & taxes à distance, assure simplicité, facilité	Jibaya'tic qui offre une meilleure traçabilité et maîtrise des échanges avec l'Administration Fiscale un suivi précis	fiscaux en ligne, 24h/24 et 7j/7, sans déplacement Qassimatouka, est dédiée au paiement en ligne de
Existe-t-il une politique pour la gestion des risques de sécurité si ?	Nous ne disposons pas d'une politique pour la gestion des risques de sécurité des systèmes d'informations seule une charte de sécurité a été mise en place	Actuellement, nous ne disposons pas d'une politique de la gestion des risques de sécurité si clairement définie et formalisée il existe seulement une politique générale de sécurité des systèmes d'information	À ce jour, la direction ne dispose pas d'une politique formalisée et documentée pour la gestion des risques de sécurité des systèmes d'information. Ce qui existe actuellement se limite à une Charte de sécurité générale, sans déclinaison opérationnelle ni niveau de détail suffisant pour encadrer efficacement les risques.
Quels sont les incidents auxquels le système d'information de la direction fait face ?	Il convient d'abord de les classer en deux catégories : les incidents fonctionnels et les incidents de sécurité. Les incidents fonctionnels sont liés au fait que les agents rencontrent des difficultés à comprendre les instructions, à maîtriser leurs tâches, ou encore aux non-conformités des bonnes pratiques préalablement établies. Cela peut	Ces incidents sont en grande partie dus au facteur humain, que ce soit par négligence laisser les portes des salles serveurs ouvertes, ou ne pas respecter les conditions adéquates telles que la climatisation et la sécurisation des accès des erreurs dans l'application des procédures d'autres types d'incidents liés	Système d'information peuvent être classés en deux grandes catégories les incidents fonctionnels et les incidents de sécurité Les incidents fonctionnels sont généralement liés au comportement des utilisateurs : incompréhension des procédures, non-respect des bonnes communication

	également inclure des situations où l'information correcte n'est pas fournie au moment opportun.	à des facteurs naturels et environnementaux, indépendants du contrôle humain	pratiques, défaillante ou encore de l'information au bon moment. Sont majoritairement d'origine externe
Quelles sont les garanties de sécurité, sauvegarde et récupération des données fiscales dans le système d'information ?	La sauvegarde des données Fiscales, la direction a établi Des sauvegardes périodiques À travers des équipements spécifiques SAN (DORADO moderne). La restauration de ces Données, une opération de test a été réalisée au niveau de la direction afin d'évaluer le temps de récupération ainsi que ses impacts. Les résultats ont montré une récupération rapide, sans coûts supplémentaires ni perte de temps	La sauvegarde des données fiscales est très importante et fait l'objet d'une grande attention au sein de la direction. Dans le cadre de notre volonté de disposer de données sécurisées et bien conservées, tous les efforts sont orientés vers la sauvegarde sécurisée et la récupération rapide des données fiscales La Direction Générale des Impôts a été renforcée par Des solutions SAN (DORADO 3000 et 6000) Qui a rendu cette opération	La sauvegarde des données Fiscales constitue une priorité Stratégique site miroir a été mis en place auprès d'Algérie Télécom, garantissant une copie Sécurisée et accessible des données à tout moment Des tests de restauration ont été conduits afin d'évaluer les délais et les conditions de récupération. Les résultats se sont révélés satisfaisants, avec une récupération rapide et sans coûts additionnels la direction a été dotée de
Quels sont les défis et les contraintes qui limitent l'efficacité de la gestion des risques au sein de la direction ?	Les enjeux qui entravent l'efficacité de la gestion des Risques sont, dans la plupart des cas, liés au facteur humain Malgré le soutien de la haute	La gestion des risques peut faire face à plusieurs défis le plus important reste la faiblesse du partage d'informations entre les Différentes parties prenantes	Acteurs freinent l'efficacité de la gestion des risques au sein de la direction le facteur humain : malgré l'engagement de la hiérarchie, Certaines parties prenantes ne jouent pas pleinement leur rôle dans ce

	Direction, les autres parties prenantes ne parviennent pas toujours à s'accorder pour assurer la réussite du processus de gestion des risques le manque de certaines compétences peut limiter cette démarche, étant donné qu'il s'agit d'un processus complexe nécessitant des	Impliquées dans le processus le manque de communication interne et l'insuffisance dans la définition précise des rôles donné qu'elle repose sur la coordination et l'alignement des différents acteurs	processus le manque de communication interne et la faiblesse du partage d'information entre les différents acteurs impliqués, ce qui nuit à la coordination nécessaire à une Gestion des risques efficace L'insuffisance de compétences
Quelles sont vos perspectives d'avenir concernant le développement de la sécurité du système d'information et l'amélioration de la gestion des risques au sein de la direction ?	La réalité, le décret présidentiel n° 07-26, publié le 5 janvier 2026, relatif à la structure de sécurité des systèmes d'information un avenir prometteur pour la gestion des risques au sein de la Direction Générale des Impôts ainsi que dans l'ensemble institution publiques une étape très importante vers la mise en place d'un cadre global définissant et structurant un processus clair et bien établi	Malgré l'absence d'une gestion des risques clairement définie, formalisée et documentée, nous restons optimistes quant à un avenir prometteur en matière de développement Cette évolution commence avec le Comité sectoriel de sécurité, qui encadre L'ensemble des institutions intervenant dans le secteur, notamment les finances, les impôts, les banques, les douanes, les domaines de l'État, sociale	Un développement notable. Cela s'explique par l'émission d'une instruction du ministère des Finances exigeant que chaque direction relevant de ce ministère la Direction Générale des Impôts, crée une direction dédiée à la sécurité des systèmes d'information. Cette direction sera chargée de tout ce qui concerne la protection et la sécurité, sous la responsabilité d'un responsable de la sécurité Il relève d'autorités des sécurité supérieures

Source : réalisé avec NVIVO

ANNEXE D:

TABLEAU COMPARATIF COMPLET DES OUTILS GRC

Critère	Archer	CISO Assistant	SimpleRisk
Modèle de licence	Payant (SaaS/On-Prem)	Open Source (AGPL v3) + Payant	Open Source + Payant
Prix	Sur devis - Très élevé	Gratuit (Community) + Payant pour le support	Gratuit + Options payantes
Architecture technique	Intégrée à multiples systèmes de sécurité	Microservices, Docker, Python	PHP/MySQL (Traditionnel)
Support des référentiels	Large (FISMA, NIST)	70+ cadres (le plus large)	Limité (NIST basique)
Support EBIOS RM	Non supporté	Support excellent	Non supporté
Support NIST	Support complet	Supporté (complet)	Supporté (800-30 basique)
Support ISO 27001	Supporté	Supporté	Supporté
Support des normes françaises	Non supporté	ANSSI, HDS, SecNumCloud, RGS	Non supporté

Critère	Archer	CISO Assistant	SimpleRisk
Support des normes américaines	FISMA, OMB, FedRAMP	Limité	Limité
MFA obligatoire	Disponible	Intégré et obligatoire	Option payante
RBAC (Gestion des droits)	Très avancé	Avancé	Basique (payant pour avancé)
SSO (SAML/OIDC)	Disponible	Disponible	Option payante
Installation On-Premise	Disponible	Complète (Docker)	Disponible (facile)
Souveraineté des données	Élevée	Totale (AGPL)	Élevée
Personnalisation	Difficile	Totale (Open Source)	Limitée
Flexibilité technique	Faible	Très élevée (Microservices)	Moyenne
Facilité d'installation	Difficile	Moyenne (nécessite Docker)	Très facile
Intelligence Artificielle	Evolv AI	(En développement)	Non disponible

Critère	Archer	CISO Assistant	SimpleRisk
Rapports et tableaux de bord	Très avancé	Avancé	Basique
Gestion des incidents	Disponible	Disponible (NIST 800-61)	Option payante
Gestion des tiers	Disponible	Disponible	Limité
Intégration avec Jira	Oui	Oui (API ouverte)	Option payante
Intégration avec ServiceNow	Oui	Possible via API	Non
Support technique	24/7	Communauté + Payant	Communauté + Payant
Documentation	Bonne	Excellente (Open Source)	Bonne
Public cible	Très grandes entreprises - Gouvernement	Gouvernement + Entreprises	Petites-Moyennes structures

Source : préparer par nous même