MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

ÉCOLE NATIONALE SUPÉRIEURE DE MANAGEMENT

ENSM. P.U. KOLÉA

MEMOIRE DE FIN D'ETUDES

MASTER EN MANAGEMENT E-GOUVERNEMENT

Management des risques d'un système d'information

Cas : CR METAL/ENCC

Élaboré par :

KHEDDOUMA Akram

Membres de jury :

Président : Mme TOUMI Djamila

Examinateur : Mme BOUZEROUTA Ilhem

Encadreur : Mme MOHAMMED EL HADJ Leila

Année 2021/2022

RÉSUMÉ

Avec l'expansion de l'utilisation des technologies de l'information (IT), la gestion des risques est la science et l'art de reconnaître l'existence de menaces, déterminer leurs conséquences sur les ressources et appliquer des facteurs modificateurs dans un manière rentable de limiter les conséquences néfastes bornes. Les stratégies de gestion des risques portent nécessairement sur une ou plusieurs processus et techniques d'analyse et traitement des risques.

La finalité de notre mémoire de master management e-gouvernement est d'examiner la gestion des risques du système d'information de CR METAL/ENCC à Blida. Pour cette raison, nous avons procédé à l'évaluation de la sécurité du SI étudié dans le but de proposer des recommandations afin d'assurer un système d'information plus sécurisé et moins vulnérable vis-à-vis les risques internes et externes.

Mots clés : Système d'Information, sécurité de l'information, Gestion des risques.

ABSTRACT

With the expanding use of information technology (IT), risk management is the science and art of recognizing the existence of threats, determining their impact on resources, and applying modifying factors in a cost-effective way to limit adverse consequences terminals. Risk management strategies necessarily relate to one or more processes and techniques for analyzing and dealing with risks.

The purpose of our master's thesis in e-government management is to examine the risk management of the CR METAL/ENCC information system in Blida. For this reason, we have carried out the security assessment of the IS studied in order to propose recommendations to ensure a more secure and less vulnerable information system against internal and external risks.

Key Words: Information system, information security, risk management.

ملخص

مع التوسع في استخدام تكنولوجيا المعلومات IT، فإن إدارة المخاطر هي علم وفن التعرف على وجود التهديدات، وتحديد تأثيرها على الموارد، وتطبيق عوامل التعديل بطريقة فعالة من حيث التكلفة للحد من العواقب السلبية النهائية. ترتبط استراتيجيات إدارة المخاطر بالضرورة بواحدة أو أكثر من العمليات والتقنيات لتحليل المخاطر والتعامل معها.

الغرض من أطروحة الماستر في إدارة الحكومة الإلكترونية هو فحص إدارة مخاطر نظام المعلومات الخاص بشركة CR METAL في البليدة. لهذا السبب، أجرينا التقييم الأمني لـ IS المدروسة من أجل اقتراح توصيات لضمان نظام معلومات أكثر أمانًا وأقل ضعفًا في مواجهة المخاطر الداخلية والخارجية.

الكلمات الدالة: نظام المعلومات، أمن المعلومات، ادارة المخاطر.

REMERCIEMENTS

En tout premier lieu, je remercie le Bon Dieu, tout puissant, de m'avoir donné la force pour survivre, ainsi que l'audace pour dépasser toutes les difficultés. Permis de mener à bien ce travail.

Pour avoir bien voulu juger ce travail bien que considéré comme un travail individuel, un mémoire ne peut pas se faire seul. C'est pourquoi je souhaite adresser des remerciements et ma gratitude aux personnes suivantes :

- Madame **Leila Mohammed El Hadj**, mon encadreur de mémoire qui m'a guidé dans mon travail et m'a aidé à trouver des solutions pour avancer.
- Monsieur **Sofiane Djiar**, pour son expertise et la pertinence de ses réponses dans le cadre du stage.
- Toutes les personnes qui m'ont soutenu et accompagné durant les études du master management e-gouvernement.

En plus de ces personnes, je souhaite également remercier toute ma famille, tant pour leur soutien moral que leur aide rédactionnelle, sans qui l'aboutissement de ce mémoire n'aurait pas pu être ce qu'il est.

Grâce à plusieurs personnes à qui nous voudrons témoigner toutes nos reconnaissances pour leur aide précieuse dans la réalisation du présent travail de recherche.

TABLE DES MATIERES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES ABRÉVIATIONS, SIGLES ET ACRONYMES

SI : Système d'Information

EBIOS : Expression des Besoins et Identification des Objectifs de Sécurité

MEHARI : Méthode Harmonisée d'Analyse de Risques

OCTAVE: Operationally Critical Threat, Asset, and Vulnerability Evaluation

ISO: International Organization for Standardization

IEC: International Standards for all electrical

ISM: Information Security Management

ISSRM: Information System Security Risk Management

COBIT: Control Objectives for Information and related Technologies

IT: Information Technology

COBIT: Control Objectives for Information and related Technologies

BDD : Base de données

DNS : Domain Name Server

IP : Internet Protocol

INTRODUCTION

Aujourd'hui, les technologies de l'information et de la communication (TIC) croissent d'une façon très rapide ce qui rend l'environnement des systèmes d'information (SI) très complexe, très turbulent, vulnérable plus exposé aux risques, moins sécurisé. Pour cela il est indispensable d'assurer une protection des SI. La gestion des risques et l'élaboration d'une politique de sécurité des systèmes d'information sont devenues plus une nécessité qu'un choix.

C'est pourquoi actuellement, la sécurité est un enjeu majeur pour les entreprises ainsi que pour l'ensemble des acteurs qui l'entourent. Elle n'est plus confinée uniquement au rôle de l'informaticien, mais aux ensembles de tous les employées et les utilisateurs. Sa finalité sur le long terme est de maintenir la confiance des utilisateurs et des clients.

De plus en plus confrontées aux problématiques de risques, les entreprises sont progressivement devenues sensibles à la nécessité d'une gestion efficace des risques, mais les risques sont de diverses natures. Dans ce travail nous nous intéressons aux risques liés aux SI des entreprises.

À cet égard, l'objectif de ce travail de recherche est de répondre à notre problématique, qui peut être formulée sous la forme de la question suivante : **comment opter pour un système d'information sécurisé (moins vulnérable) qui assure la performance organisationnelle ?**

De cette problématique découlent plusieurs sous questions. Il s'agit notamment de :

- Sous quel angle de vision il a été traité dans la littérature ?
- Comment peut-on définir le concept de gestion de risques des systèmes d'information ?
- Quels sont les outils et techniques optimales utilisés pour assurer la sécurité d'un SI ?

Tout au long de notre recherche, nous allons essayer de répondre à l'ensemble de ces questions en décomposant notre travail à trois chapitres.

Le premier chapitre est un chapitre théorique contient deux sections, la première section présente une revue de littérature et les réflexions au sujet de la sécurité de SI. Ensuite la deuxième partie présente le cadre conceptuel, qui présente tout le cadre théorique lié à notre thématique.

Le deuxième chapitre intitulé cadre méthodologique et organisationnel est consacré à définir notre position épistémologique, la méthodologie de recherche et les méthodes de collecte et d'analyse de données. Ensuite le cadre organisationnel qui se décompose en étude de cas de contexte et présentation de l'organisme d'accueil.

Le dernier volet de notre mémoire sera consacré pour l'interprétation et discussion des rapports obtenus, puis synthèse de résultats et nous finalisons par une petite recommandation.

CHAPITRE I : REVUE DE LITTÉRATURE ET CADRE CONCEPTUEL

Section 1: REVUE DE LITTÉRATURE

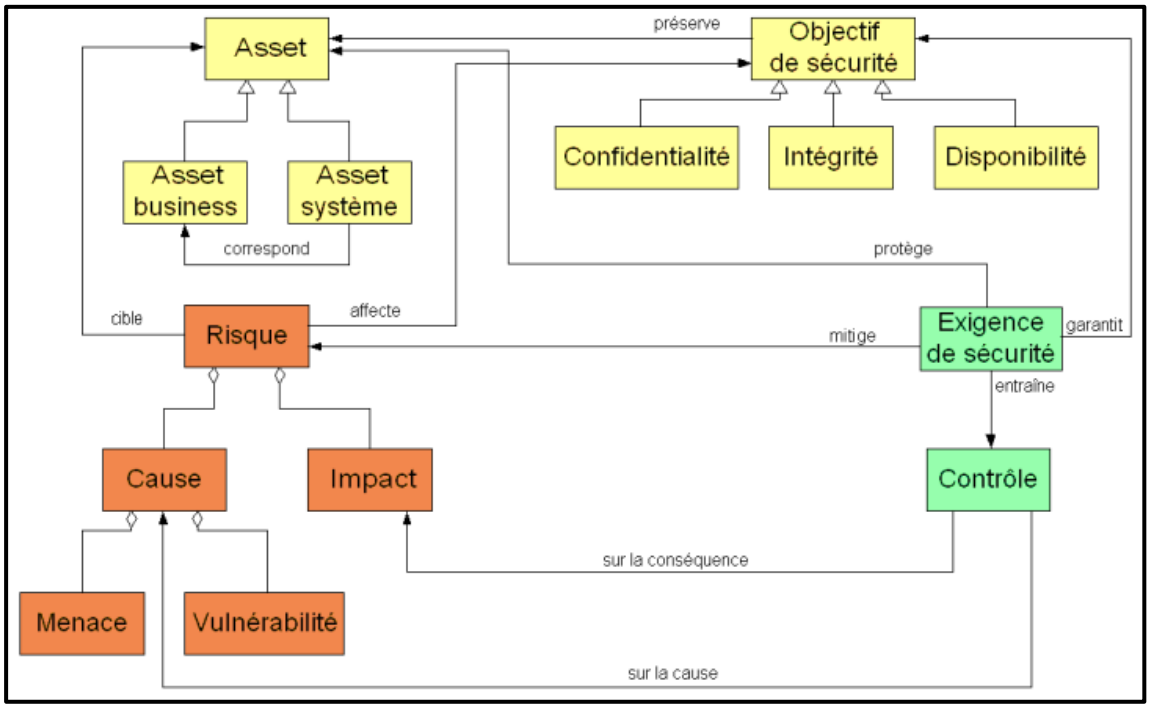
À travers la revue de littérature, nous allons mettre en évidence certains travaux qui ont traité le management des risques d'un système d'information au sein d'une entreprise.

1.1 Concept gestion des risques

(Nicolas Mayer) et **(Jean-Philippe Humbert),** Ingénieurs R&D – Centre de Recherche Public Henri Tudor – Luxembourg. Ingénieur R&D – Centre de Recherche Public Henri Tudor – Luxembourg. Ont évoqué la thématique gestion des risques des systèmes d'information, bien qu'un grand nombre ne soit plus utilisé ou confidentiel, ils estiment qu'il existe plus de 200 méthodes de gestion des risques, ils ont focalisé sur trois des principales méthodes actuellement utilisées.

Ils ont présenté les concepts de la gestion des risques dans la figure suivante :

Figure 1: concept de la gestion de risque.



Source : (MAYER, 2009).

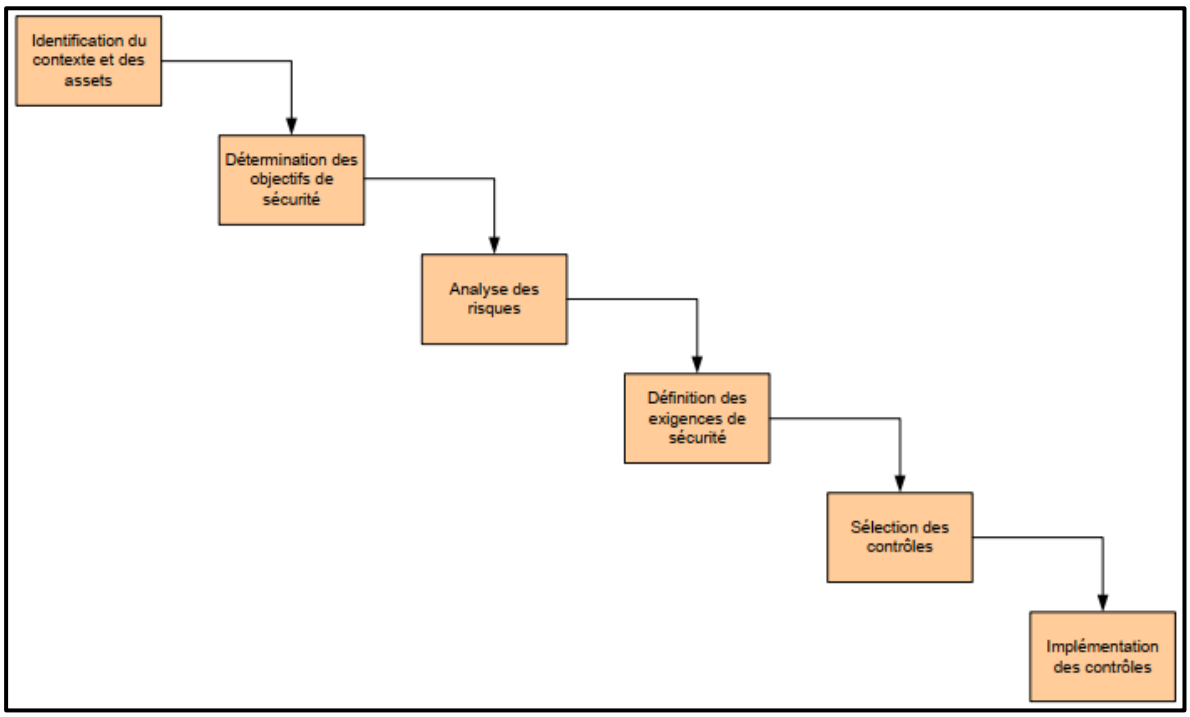
D'où ils ont défini un risque à l'aide de ce que l'on nomme « l'équation de risque », qui joue un rôle fondamental dans l'identification et l'évaluation du risque :

Risque = menace * vulnérabilité * impact

1.1.1 Processus gestion du risque

Aussi, ils ont dévoilé le processus de gestion des risques en six étapes, présenter dans le schéma suivant :

Figure 2: processus gestion de risque.



Source : (MAYER, 2009).

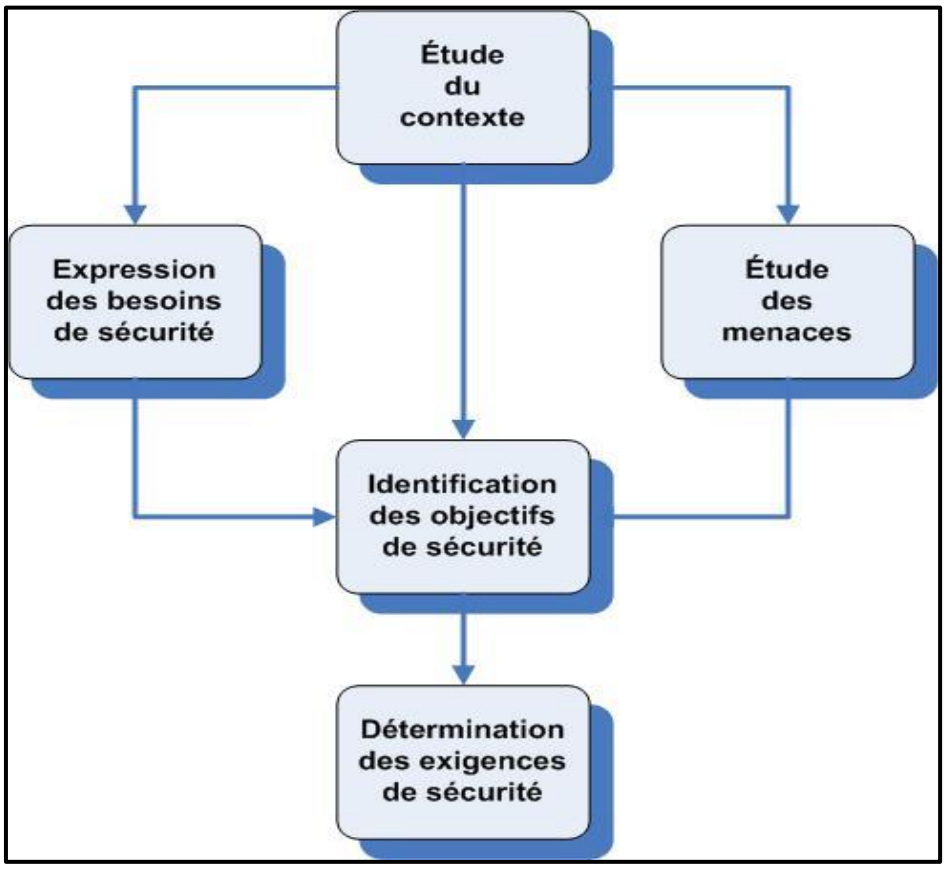
1.1.2 Méthodes de gestion des risques

Pour réduire le champ du choix au cœur des méthodes de la gestion des risques, ils ont choisi de détailler **EBIOS** (Expression des Besoins et Identification des Objectifs de Sécurité), **MEHARI** (Méthode Harmonisée d'Analyse de Risques) et **OCTAVE** (Operationally Critical Threat, Asset, and Vulnerability Evaluation).

- **EBIOS :** (Schneier, 2000) il s'agit d'une méthode développée et maintenue par la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information) crée en 1995, se compose de cinq guides (Introduction, Démarche, Techniques, Outillages pour l'appréciation des risques et Outillages pour le traitement des risques) et d'un logiciel support. La méthode a pour objectif la formalisation d'objectifs de sécurité adaptés aux besoins du système audité (et de son contexte).

Démarche EBIOS globale présentée dans la figure suivante :

Figure 3: démarche globale EBIOS.



Source : (Schneier, 2000).

Quant au processus de gestion des risques, les phases 5 et 6 vues précédemment ne sont pas réellement développées, ce qui ne permet pas de valider véritablement le cycle théorique dans son ensemble. Dans ce cas, certains considèrent alors EBIOS exclusivement comme une méthodologie d'analyse des risques.

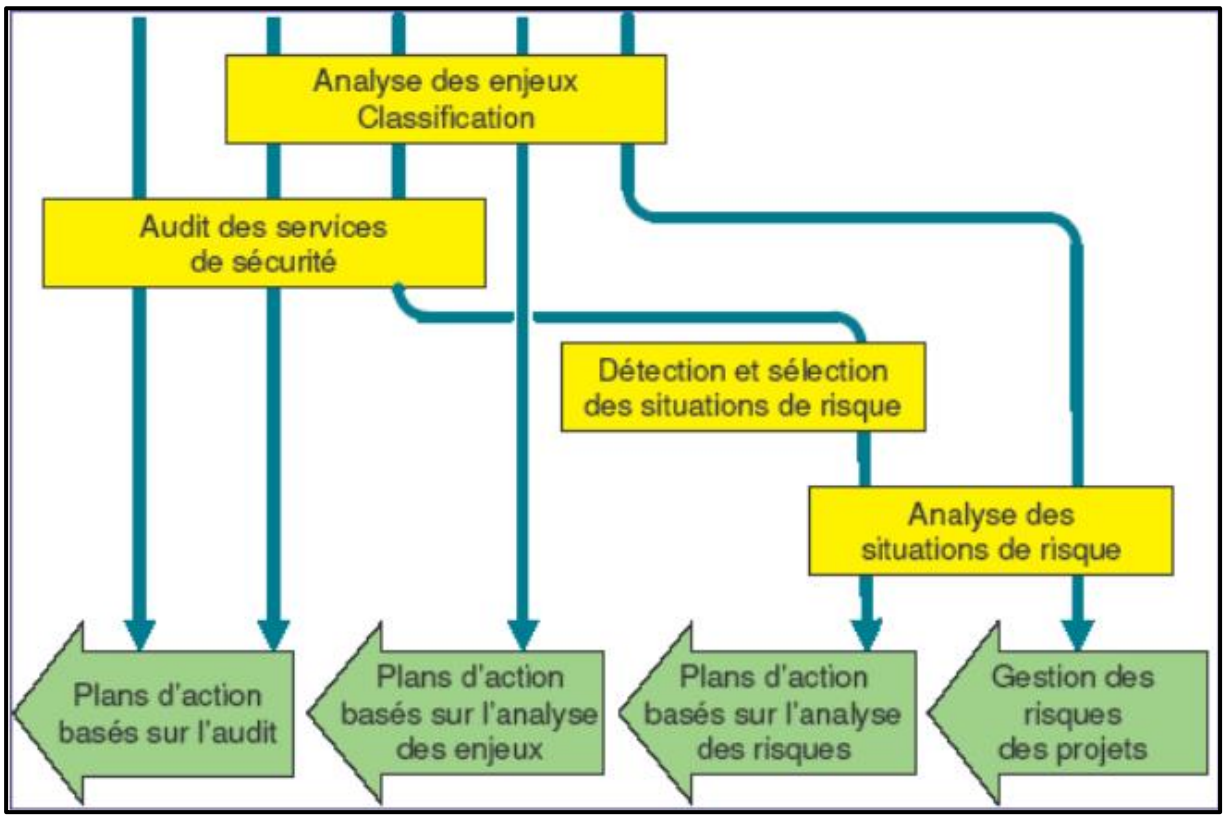
- **OCTAVE :** (Schneier, 2000) cette méthode d'évaluation du risque est publiée par le Software Engineering Institute (SEI) de la Carnegie Mellon University, reconnue dans le domaine de la sécurité des SI (fédération des Computer Emergency & Reponse Team – CERTS). Les fondements mêmes de cette méthode reposent sur la possibilité de réaliser une analyse des risques de l'intérieur de l'organisation, exclusivement avec des ressources internes. Pleinement orientée vers les grands comptes, une version OCTAVE-S (Small) peut, cependant, facilement se décliner au sein d'une petite structure économique.

Les phases principales d'OCTAVE, à savoir préparation, vue organisationnelle, vue technologique et développement de la stratégie.

- **MEHARI :** demeure une des méthodes d'analyse des risques les plus utilisées actuellement. Elle est dérivée de deux autres méthodes d'analyse des risques (MARION et MELISA). MEHARI est maintenue en France par le CLUSIF (Club de la Sécurité des Systèmes d'Information Français) (14001, 2004), via notamment le Groupe de Travail dédié à cette méthode.

Démarche MEHARI globale, est présentée dans la figure suivante :

Figure 4: démarche globale MEHARI.



Source : (Schneier, 2000).

MEHARI présente une grande diversité dans l'utilisation de ses modules. Trois approches se détachent plus particulièrement : en se basant sur analyse détaillée des risques, en se basant sur l'audit de sécurité et dans le cadre de la gestion d'un projet particulier.

1.2 Participation des utilisateurs à la gestion des risques de sécurité des SI

Janine L. Spears, université Depaul **et Henri Barki**, HEC Montréal**. Ont rédigé un article intitulé :** User participation in information systems Security risk management.

Dans leur article, Spears et Barki examinent l'implication des utilisateurs dans la gestion des risques de sécurité des systèmes d'information et son impact dans le contexte de la

conformité réglementaire à travers une étude multiméthodes au niveau de l'organisation.

En premier lieu, ils ont interrogé 11 informateurs de cinq organisations, afin de comprendre les types de contrôles de sécurité et d'activités auxquels les utilisateurs s'engagent dans le cadre de la conformité Sarbanes-Oxley et les résultats associés. Un modèle de recherche est développé sur la base des résultats de la recherche qualitative et des théories existantes sur la participation des utilisateurs dans la littérature sur le développement de systèmes.

L'analyse des données recueillies lors d'une enquête par questionnaire auprès de 228 membres de l'ISACA, une association professionnelle spécialisée dans la gouvernance, l'audit et la sécurité des IT, a soutenu le modèle de recherche. Les résultats des deux études convergent et montrent que l'engagement des utilisateurs contribue à améliorer les performances des contrôles de sécurité grâce à une plus grande sensibilisation et un meilleur alignement entre la gestion des risques de sécurité informatique et l'environnement commercial, tout en développant de meilleurs contrôles. Alors que la littérature sur la sécurité des SI décrit souvent les utilisateurs comme le maillon le plus faible de la sécurité, les recherches actuelles suggèrent que les utilisateurs peuvent être une ressource importante pour la sécurité des SI en apportant les connaissances métiers nécessaires pour contribuer à des mesures de sécurité plus efficaces. L'engagement des utilisateurs est également un moyen d'inciter les utilisateurs à protéger les informations sensibles dans leurs processus métier et améliorer l'élaboration de mesures de contrôle.

1.3 Défis actuels en gestion des risques de la sécurité de l’information

Stefan Fenz and Johannes Heurix, Department of Research for consistency, Vienna University of Technology and SBA Research, Vienna, Austria.

Thomas Neubauer, Department of Science and Technology Management, Xylem Technologies, Vienna, Austria.

Fabian Pechstein, Department of Research for consistency, Vienna University of technology and SBA Research, Vienna, Austria.

Le but de leur article intitulé **Current challenges in information security risk management**, est de donner un aperçu des approches actuelles de gestion des risques et décrire leurs points communs et leurs différences, évaluer les approches actuelles de gestion des risques concernant leur capacité à prendre des décisions rentables sans sécurité inutile compromis. Esquisser les problèmes fondamentaux actuels de la gestion des risques à partir

du retour d'expérience industriel et littérature académique et fournir des solutions potentielles et des orientations de recherche pour répondre aux problèmes identifiés. Malgré des décennies de recherche, le domaine de la gestion des risques liés à la sécurité de l'information est toujours confronté à de nombreux défis qui empêchent les gestionnaires de risques d'obtenir des résultats solides en matière de gestion des risques.

L'article de recherche **Current challenges in information security risk management** fournit un point de référence aux professionnels et aux chercheurs en synthétisant les enjeux actuels dans le domaine de la gestion des risques en sécurité de l'information. Par conséquent, les résultats permettent aux chercheurs de concentrer leur travail sur les défis du monde réel identifiés et ainsi contribuer à faire progresser le domaine de la gestion des risques liés à la sécurité de l'information de manière structurée.

Les praticiens peuvent aussi utiliser les résultats de la recherche pour identifier les faiblesses communes et les solutions potentielles dans programmes de gestion des risques liés à la sécurité de l'information.

- **Conception/méthodologie/approche :**

Stefan Fenz and Johannes Heurix, Thomas Neubauer et Fabian Pechstein ont identifié les enjeux de la gestion des risques de sécurité de l'information, les approches existantes sont comparées les unes aux autres, et en conséquence, une méthodologie abstraite est dérivée pour aligner l'identification du problème et de la solution sur ses phases génériques. Les défis ont été identifiés sur la base d'enquêtes bibliographiques et des commentaires de l'industrie.

- **Résultats :**

En tant que problèmes courants lors de la mise en œuvre de la gestion des risques de sécurité de l'information approches, nous avons identifié les domaines de l'inventaire des actifs et des contre-mesures, l'affectation de la valeur des actifs, prédiction, l'effet d'excès de confiance, le partage des connaissances et le risque versus. La revue des approches de gestion de risques ne fournit pas explicitement de mécanismes pour aider les décideurs à prendre des décisions. Un compromis risque/coût approprié, mais nous avons identifié des approches académiques qui répondent à ce besoin.

1.4 Gestion des risques des SI et performance organisationnelle

(Lahoucine IKKOU, 2016), Chercheur à la Faculté des Sciences Juridiques, Economiques

et Sociales, Université IBEN ZOHR-AGADIR.

(Abdelkbir ELOUIDANI, 2016), professeur à la Faculté des Sciences Juridiques, Economiques et Sociales, Université IBEN ZOHR-AGADIR.

Ils Ont rédigé un article sur la gestion des risques des systèmes d'information dans les organismes publiques au Maroc. D'après eux la sécurité des SI recouvre un ensemble de méthodes, technologies et outils chargés de protéger les ressources d'un SI afin d'assurer : la disponibilité des services, la confidentialité des informations, l'intégrité des systèmes, traçabilité et la conformité.

L'objectif de cet article est d'expliquer comment, d'une part à travers la théorie, la gestion des risques de systèmes d'information peuvent apparaître comme l'un des déterminants de la performance au sein d'une organisation publique et d'autre part à travers une étude sur les organisations publiques au Maroc.

Suivant leur problématique : **quels bénéfices de la gestion des risques SI peuvent apporter à la performance organisationnelle ?** En effet, suivant leur étude empirique ils ont abordé d'abord lieu d'analyse descriptive, puis l'analyse exploratoire (ACP : Analyse des composantes principales et ACM : Analyse en correspondance multiple) et enfin l'analyse confirmatoire, **Lahoucine IKKOU et Abdelkbir ELOUIDANI** ont constaté que la gestion des risques des systèmes d'information pourrait contribuer à la performance au sein des organisations publiques vu la relation significative entre eux (la gestion des risques améliore la performance organisationnelle).

Pour conclure, d'après cet article nous déduisons la liaison de gestion des risques avec la performance organisationnelle, ce implique forcément la nécessité primordiale de sécurisé le SI et le rendre moins vulnérable.

1.5 Gestion des systèmes d'information ISM

(Ronald E. McGaughey, 1994) Professeur au Département des systèmes d'information et des sciences de la décision à l'Université technologique de l'Arkansas.

(Charles A. Snyder, 1994) Professeur et chef de département de la gestion à l'Université d'Auburn.

(Houston H. Carr, 1994) Professeur agrégé de gestion (MIS) et directeur associé du Thomas Centre Walter pour la gestion de la technologie à l'Université d'Auburn.

Dans leur livre **(Information & Management 26 1994, pages 273-280)**, ils ont constaté que les stratégies de gestion des risques doivent être intégrées à la planification stratégique des SI. L'identification, la classification et la compréhension des risques SI, peut être facilité par l'utilisation de l'analyse de la chaîne de valeur. Juste, car cela peut aider une entreprise à identifier d'autres utilisations de IT qui peut offrir un avantage concurrentiel prometteur, il peut également aider à identifier les risques informatiques qui devrait être pris en compte dans l'évaluation des alternatives usages de l'informatique. La chaîne de valeur peut également aider à déterminer où les expositions au risque pur existent avec au regard de l'informatique actuelle.

Aussi, ils ont jugé dans leur livre que certains outils sont utiles pour évaluer les risques spéculatifs, d'autres pour les risques purs. Les entreprises devraient utiliser les outils appropriés et les responsables informatiques doivent être familiarisés avec les outils et les approches du risque analyser et savoir quand et comment les appliquer.

1.6 Gestion de risques des systèmes d'information ISRM

(Mohamed S. Saleh,2011) assistant Professor of Information Systems, Imam Mohamed ibn Saud University.

(Abdulkader Alfantookh, 2011) Prof. of Intelligent Control Systems.

Article **A new comprehensive framework for enterprise information security risk management** dans le journal Applied **Computing and Informatics.**

Leur article a présenté un nouveau cadre ISRM d'entreprise qui bénéficie d'une fonctionnalité pour une utilisation future. Le cadre de la portée avec cinq domaines (stratégie, technologie, organisation, personne, et l'environnement) lui permet de prendre en charge le large éventail de problèmes associés à l'ISRM, d'une manière bien structurée et ouverte. Cela intègre non seulement les problèmes qui ont été pris en compte par d'autres méthodes, mais permet également de prendre en compte d'autres problèmes ou des problèmes émergents.

Aussi, ils ont présenté le processus du module six-sigma. Qui permet d'accueillir divers processus d'autres méthodes ISRM dans une méthode unifiée et largement acceptée.

En outre, le cadre répond à la nécessité d'utiliser une gestion critères, et permet de prendre en compte différents critères, dont ISO contrôles de sécurité de l'information et en tenant

compte de critères de référence prédéterminés.

ISRM envisage également l'utilisation d'outils pour effectuer les différentes phases du processus de manière efficace, comme c'est le cas avec d'autres méthodes ISMR.

D'après **Mohamed S** et **Abdulkader Alfantookh,** la nature complète et flexible du cadre en fait un candidat pour devenir une « référence ouverte » pour l'ISRM qui peut être largement utilisée par les entreprises à la recherche de sécurité environnement pour leur entreprise basée sur l'e-commerce.

1.7 Gestion des risques de SI d'entreprises françaises

(Caroline Aubry) Maître de conférences, Université Toulouse III - Laboratoire Gestion et Cognition, a abordé la gestion des risques dans les entreprises françaises (état des lieux et émergence d'une approche cognitive et organisationnelle). Dont l'objectif de savoir où en sont les entreprises françaises face aux risques et leur gestion, d'en proposer une approche globale intégrant la dimension cognitive.

D'après **(Caroline Aubry),** l'état des lieux sur le risque et leur gestion est nécessaire pour appréhender la situation dans les entreprises françaises. Il ressort par ailleurs des études menées sur le terrain et des témoignages de professionnels - et c'est l'aspect novateur de son approche - qu'au-delà du discours « désincarné » de certains *risk-managers* et de la vision statique, souvent limitée à l'énoncé des différentes étapes et outils à mettre en œuvre, la mise en place d'une démarche globale et dynamique de gestion des risques ne va pas de soi.

Aussi, elle a mentionné qu'une première perspective pourrait être de repérer dans quelques entreprises ciblées les points forts et les insuffisances des systèmes existants en matière de gestion des risques, les bonnes pratiques ainsi que les moins bonnes et surtout, dans la mesure où il s'agit de questions 19 dynamiques où l'implication des acteurs est essentielle, de repérer les moteurs et les freins du développement des démarches mises en œuvre. Cette première étape encore très orientée vers l'identification technique des risques devrait être complétée par une réflexion plus globale intégrant la dimension cognitive[31]. Cette deuxième perspective pourrait conduire à mettre en place des systèmes organisationnels et managériaux qui favorisent par exemple la responsabilisation des personnes et des groupes ou encore l'auto - production de solutions et à définir, à partir d'observations pratiques, de leur critique et d'une ingénierie spécifique, des modalités d'évaluation et d'amélioration de ceci. L'enjeu est de permettre l'appropriation de la prévention des risques opérationnels par

les acteurs et de favoriser sa mise en œuvre ainsi que la montée en compétences des acteurs.

1.8 Système d'information et performance organisationnelle

La relation entre le système d'information et la performance de l'entreprise a fait l'objet de plusieurs travaux, mais reste d'actualité dans les recherches en management et l'impact des SI et des technologies sur la performance demeure une question. Certaines études ont montré la relation positive et significative et (Nwamen, 2006) montre que l'utilisation du SI et Tic influence positivement la performance commerciale et a constaté l'augmentation de certains indicateurs commerciaux (chiffre d'affaires, parts de marché, qualité des produits offerts).

Les résultats de (Alaoui, 2010) confirment qu'il est difficile d'évaluer l'impact des Tic et SI sur la performance de l'entreprise bien que celle-ci gagne en rapidité et en adaptabilité en intégrant dans son organisation des SI, lorsque ceux-ci sont mis au service de la stratégie opérationnelle de l'entreprise et que les SI intégrés permettent d'enrichir les pratiques managériales de l'entreprise et facilitent le partage de l'information. D'autre part, il remarque que l'usage des SI par l'entreprise permet de produire des effets positifs sur l'évolution à long terme du chiffre d'affaires et des coûts de transport de la société MBA-rance. Cependant, le lien entre le SI, Tic et performance est négatif dans certains cas et cela se justifie par le choix des approches méthodologiques et les contextes dans lesquels les études se sont déroulées (Deltour & Lethiais, 2014).

Section 2: CADRE CONCEPTUEL

Dans cette partie du mémoire, nous allons mettre les points sur tout qui concerne le système d'information, la gestion de la sécurité des SI (concept et impact sur la performance organisationnelle) et management des risques des SI.

2.1 Système d'information

Le concept système d'information se compose de deux termes importants (MAHARRAR, 2014) :

- **Système** : Un système est un ensemble d'éléments interdépendants contenus dans un ensemble plus vaste. En latin et en grec, le mot « système » signifie combiner, établir, réunir. Un sous-système est un système qui fait partie d'un autre système. Typiquement, un système se compose de composants (ou d'éléments) organisés ensemble pour faciliter la circulation de l'information, de la matière ou de l'énergie.
- **Information** : est un ensemble de données, reçues par la personne qui les interprète. C'est aussi un élément de connaissance qui peut être codé pour le stockage, le traitement ou la communication.

Il n'est pas aisé de donner une définition pertinente et pratique d'un système d'information, car les chercheurs en ont donné plusieurs définitions et nous nous y référons plus haut.

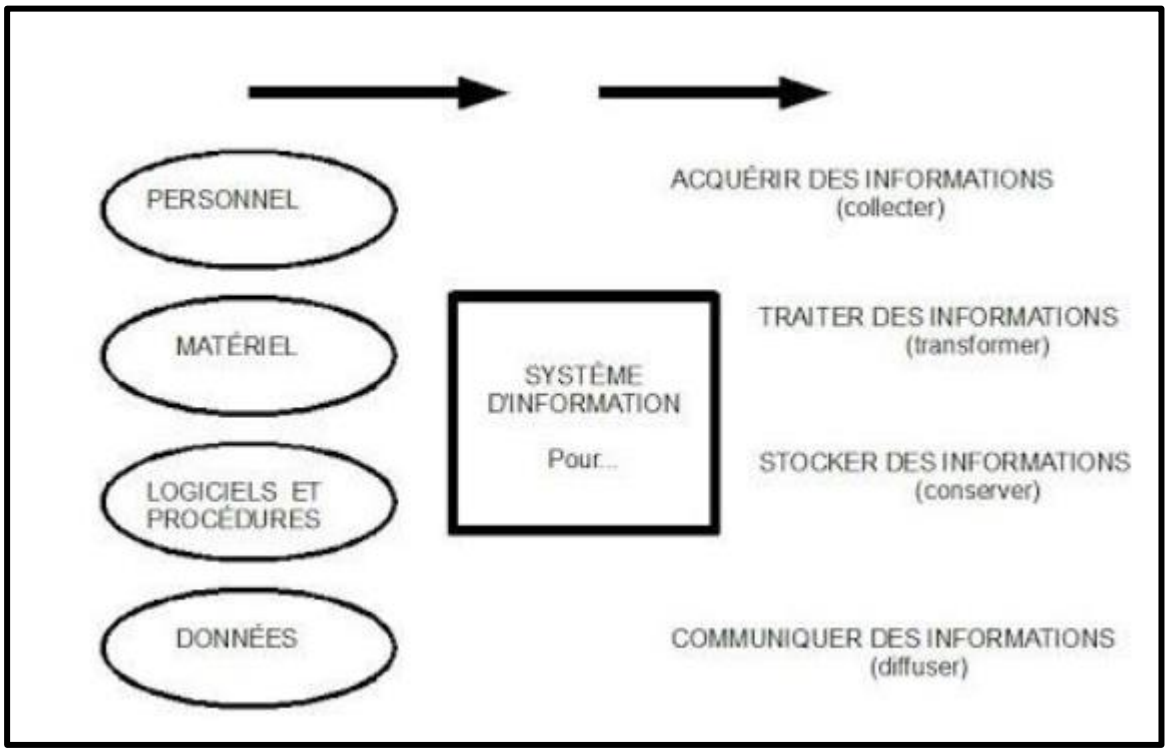
2.1.1 Définitions d'un système d'information

SI est l'interface entre les autres systèmes de l'entreprise. Il sert le système d'exploitation chargé de collecter les données liées à ses activités. Il représente un moyen d'exploitation d'une application définie par une structure technique (contrôle de gestion, management de la qualité), (Gillet & Gillet, 2013).

SI comme un ensemble de ressources (matériels, logiciels, données, procédures, humains ...) structurées pour acquérir, traiter, mémoriser, transmettre et rendre disponible l'information (sous forme de données, textes, sons, images...) dans et entre les organisations, (Reix, Fallery, Kalika, & Rowe, 2016).

Un système d'information est un ensemble intégré et cohérent de logiciels dirigés par les technologies de l'information qui supportent les individus, les organisations et les objectifs sociétaux, (Waston, 2008).

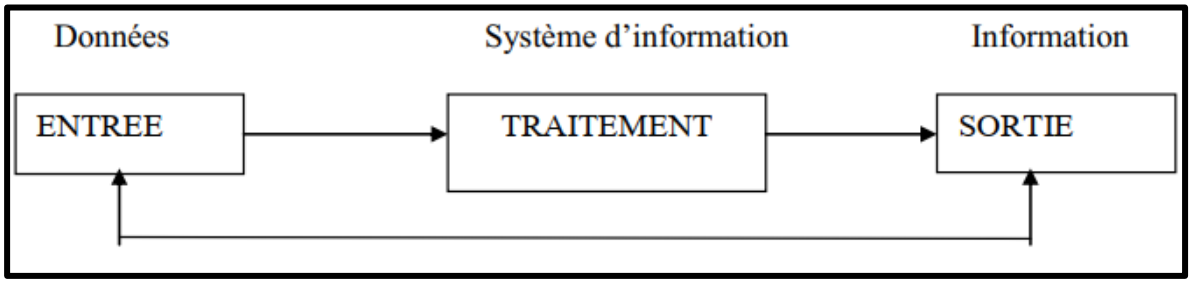
Figure 5: Le système d'information selon Reix.



Source: (Reix, Fallery, Kalika, & Rowe, 2016).

Dans un système d'information, il y a trois activités principales qui aident à la production de l'information à l'organisation : l'entrée, le traitement et la sortie.

Figure 6: les fonctions d'un système d'information.



Source : (Kenneth & Jane, 2006).

L'**Entrée**, est le processus au cours duquel les données brutes sont fournies au système en provenance de l'organisation ou de son environnement. Ce processus peut prendre des formes différenciées.

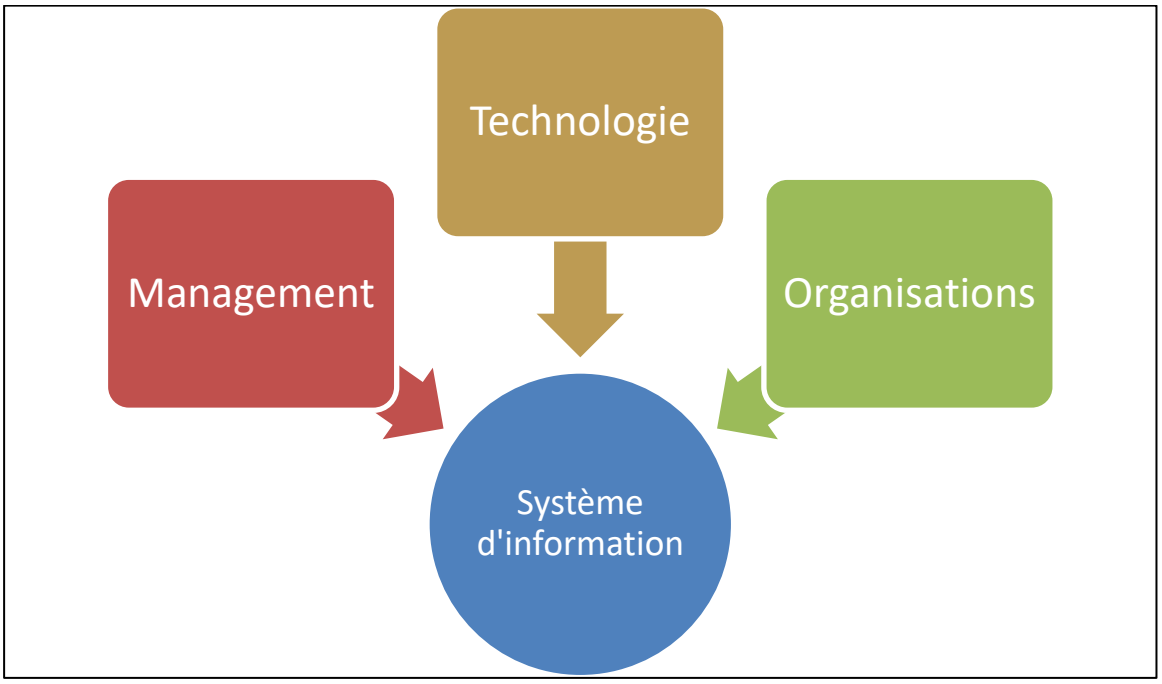
La Sortie, est le processus de diffusion de l'information traitée aux utilisateurs qui ont besoin. Les informations une fois traitées doivent être mises à la disposition de l'utilisateur

final. Ces trois activités peuvent être enchainées en quelques secondes (en « temps réel ») ou réalisées de manière asynchrone (en « temps différé »).

2.1.2 Dimensions d'un système d'information

(Laudon & Laudon, 2013) insistent sur le fait qu'il n'est pas possible de considérer un SI exclusivement sous l'angle technologique. Ils en déduisent le schéma ci-dessous que nous allons illustrer en nous appuyant sur la lecture « processus ».

Figure 7: dimensions du système d'information



Source : Management des systèmes d'information (Laudon & Laudon, 2013)

- **Dimension organisationnelle**

L'activité peut souvent être schématisée par nombre de processus plus ou moins interdépendants avec des étapes dont certaines apportent de la valeur ajoutée et d'autres non. Il s'agit de flux de données, de matières, de décisions, etc. qui peuvent être pensés en utilisant les techniques de réingénierie d'affaires (Hammer, 1990). Le résultat débouche souvent sur la mise en place d'une technologie s'appuyant sur un logiciel workflow qui va permettre de modéliser et d'automatiser les flux d'informations dans l'organisation.

- **Dimension managériale**

Le flux de données est une ressource fondamentale pour chaque manager, lequel est

destinataire « pour information », « pour avis » ou « pour décision » (Laudon & Laudon, 2013). Ainsi, il est possible de voir que le rôle du management est essentiel pour réussir l'implémentation d'un tel outil et que l'activité elle-même de chaque manager en sera fortement impactée.

- **Dimension technologique**

Cette dimension est souvent considérée dans les faits comme le plus important, car des présupposés organisationnels ont servi à bâtir l'outil. Par ailleurs, les adaptations organisationnelles seront marginales et seront prises en compte lors d'un simple paramétrage.

2.2 Gouvernance d'un système d'information

Le terme Gouvernance désigne la capacité d'une organisation d'être en mesure de contrôler et de réguler son propre fonctionnement afin d'éviter les conflits d'intérêts liés à la séparation entre les ayants droit (actionnaires) et les acteurs. Selon (Pérez, 2003) *« la gouvernance d'entreprise se réfère aux dispositifs institutionnels et comportementaux régissant les relations entre les dirigeants d'une entreprise et ses stakeholders »*. La gouvernance du système d'information est un principe dérivé de la gouvernance d'entreprise qui porte sur la façon de gérer et d'administrer le système d'information de l'entreprise pour qu'il puisse contribuer à la création de valeur. La préservation et le développement des biens immatériels, ainsi que la traçabilité et le contrôle des données financières, entrent dans ce cadre (Bohnké, 2010). La gouvernance du SI est vue comme un processus de management, fondé sur de bonnes pratiques, qui permet à l'entreprise d'optimiser ses investissements en système d'information dans le but d'atteindre un ensemble d'objectifs (contribuer à ses objectifs de création de valeur, accroître la performance des processus informatiques et leur orientation client, maîtriser les aspects financiers du système d'information, développer les solutions et les compétences en système d'information dont l'entreprise aura besoin dans le futur, garantir que les risques liés au système d'information sont sous contrôle) tout en développant la transparence (Leignel, 2006).

En réponse à la volonté d'exercer une bonne gouvernance des SI, COBIT s'attache aux cinq axes stratégiques, considérés comme les domaines de gouvernance de SI (Moisand & De Labareyre, 2009):

- **L'alignement stratégique :** Consiste à s'assurer que les plans informatiques

restent alignés sur les plans des métiers, à définir, tenir à jour et valider les propositions de valeur ajoutée de l'informatique, à aligner le fonctionnement de l'informatique sur le fonctionnement de l'entreprise.

- **L'apport de valeur :** Consiste à mettre en œuvre la proposition de valeur ajoutée tout au long de la fourniture du service, à s'assurer que l'informatique apporte bien les bénéfices attendus sur le plan stratégique, à s'attacher à optimiser, les coûts et à prouver la valeur intrinsèque des SI.
- **La gestion des risques :** Exige une conscience des risques de la part des cadres supérieurs, une vision claire de l'appétence de l'entreprise pour le risque, une bonne connaissance des exigences de conformité, de la transparence à propos des risques significatifs encourus par l'entreprise et l'attribution des responsabilités dans la gestion des risques au sein de l'entreprise.
- **La gestion des ressources :** Consiste à optimiser l'investissement dans les ressources informatiques vitales et à bien les gérer les applications, informations, infrastructures et personnes. Les questions clés concernent l'optimisation des connaissances et de l'infrastructure.
- **La mesure de la performance :** Consiste en un suivi et une surveillance de la mise en œuvre de la stratégie, de l'aboutissement des projets, de l'utilisation des ressources, de la performance des processus et de la fourniture des services, en utilisant par exemple des tableaux de bord équilibrés qui traduisent la stratégie en actions orientées vers le succès d'objectifs mesurables autrement que par la comptabilité conventionnelle.

Figure 8: Les domaines de gouvernance du SI

Source : Élaborée par nous-mêmes.

2.3 Sécurité de l'information

L'information est un actif critique qui est devenu le quatrième facteur économique à côté des ressources humaines, naturelles et du capital. Aujourd'hui la recherche insiste sur la protection de l'information en garantissant les trois aspects clés de la sécurité (confidentialité, intégrité, disponibilité).

En somme, le besoin sécurité de l'information « est comme l'oxygène ; quand vous l'avez, vous le prenez, mais quand vous ne l'avez pas, l'obtenir devient la priorité immédiate et serrante », cette analogie par **(Joseph Nye, université de Harvard).**

La sécurité vise à protéger la confidentialité, l'intégrité et disponibilité des informations et/ou des processus dans une organisation :

- **Confidentialité :** est la propriété que l'information ne soit pas rendue disponible ou divulguée à des personnes, entités ou processus non autorisés ;
- **Intégrité :** est la propriété de sauvegarder l'exactitude et l'exhaustivité des actifs. L'exactitude pourrait être menacée par une mise à jour (non autorisée ou indésirable) ou falsification. L'exhaustivité pourrait être menacée par la modification ou la suppression ;

- **Disponibilité :** est la propriété d'être accessible et utilisable à la demande par un entité autorisée.

D'autres critères comme l'authenticité, la non-répudiation ou la responsabilité pourraient être ajoutés lorsque le contexte l'exige, mais ils sont généralement considérés comme secondaires.

2.4 Gestion des risques des SI

Concept de gestion des risques a très certainement fait son apparition à la fin des années 50 aux États-Unis dans le domaine financier, en relation avec des questions d'assurance (GREMBO, 2020).

Par la suite, la notion de gestion des risques a été étendue à d'autres domaines, citons notamment l'environnement, la gestion de projet, le marketing, ainsi que la sécurité informatique, qui m'intéresse tout particulièrement.

La gestion des risques de sécurité liés aux SI est définie par l'ISO (Avanesov, 2009) comme l'ensemble des activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque. On dégage en général trois finalités à la gestion des risques pour les SI :

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

2.4.1 Risque de sécurité de l'information

Possibilité qu'une menace donnée exploite les vulnérabilités d'un actif ou d'un groupe d'actifs et nuise donc à l'organisation. Le risque est mesuré en termes de combinaison entre la vraisemblance d'un événement et ses conséquences.

2.4.2 Types de risques

Selon (Crockford, 1980), les grandes catégories de risques sont :

- **Incendies et catastrophes naturelles :**
  Les plus évidentes menaces pour les biens et les revenus de l'entreprise.
- **Accident :**
  Décès ou blessure du personnel clé et/ou atteinte aux actifs, etc.
- **Politique et social :**

Elles sont parfois liées au changement.

- **Technique :**
  Associés à l'adoption ou non du changement technique.
- **Marketing :**
  Réponse à une organisation produits et efforts promotionnels.

Aussi d'après (Doherty, 1985), les risques peuvent également être classés comme **assurables** et **risques non assurables**. Les risques assurables peuvent être souscrits, en transférant le coût des conséquences néfastes à un tiers.

Les risques peuvent également être classés comme **ancien**s ou **nouveaux** (Crouch & Wilson, 1982)**.** Les anciens risques sont associés aux événements qui se sont produits et peuvent continuer à se produire. Des données sont souvent disponibles pour les analyser. Les nouveaux risques et les événements qui les provoquent peuvent avoir s'est produit auparavant, mais l'a fait sans être observé. Ils posent des défis uniques pour responsables de la gestion des risques.

Aussi selon (MAKHLOUF SHABOU, 2018), les types de risques sont :

- Risque opérationnel et stratégique ;
- Risque interne/externe ;
- Risque financier ;
- Risque juridique ou de conformité ;
- Risque environnemental, climatique ou naturel ;
- Risque IT, SI, informatique ou technologique ;
- Risque humain ou lié au RH ;
- Risque politique ou géopolitique ;
- Risque économique ;
- Risque de réputation ou d'image ;
- Risque informationnel.

2.4.3 Gestion des risques

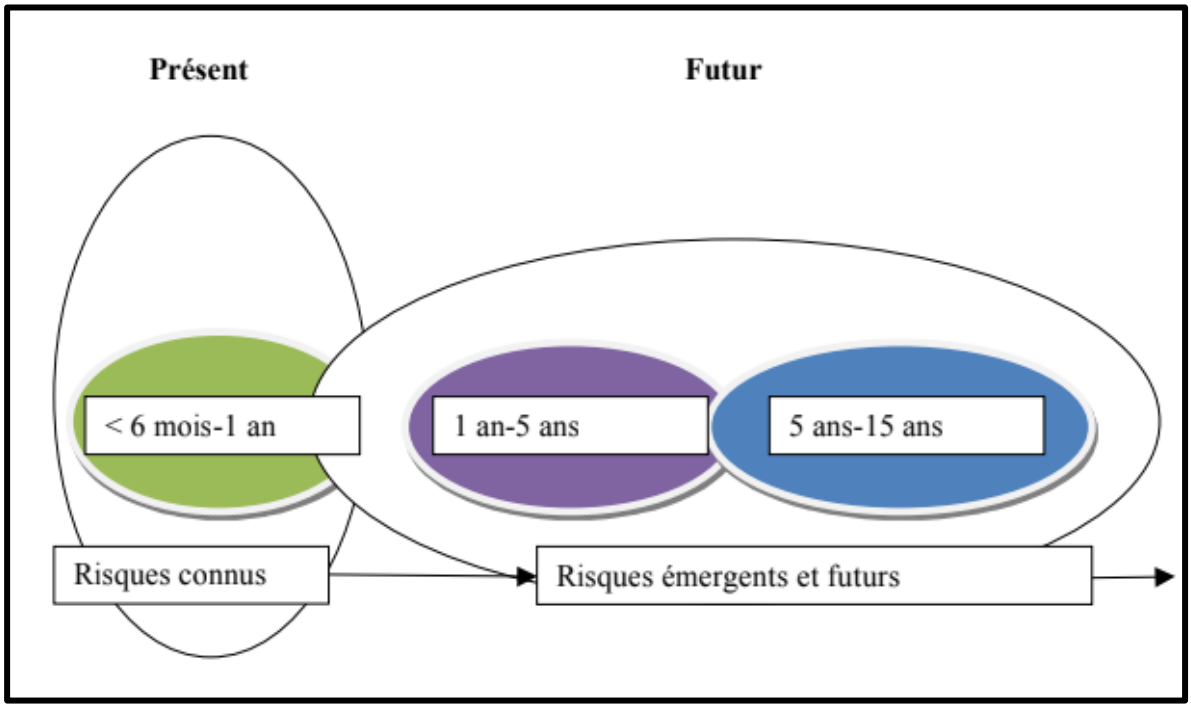
La gestion des risques est la science et l'art de reconnaître l'existence de menaces, déterminer leurs conséquences sur les ressources, et en appliquant modifier les facteurs de manière rentable pour garder les conséquences néfastes dans les limites. La prise de décision en matière de risque doit se concentrer sur les identifier, les mesurer et les manipuler

(McGaughey, Snyder, & Carr, 1994).

Les stratégies de gestion des risques une ou plusieurs des composantes des risques : menaces, ressources, les facteurs modificateurs et les conséquences. La stratégie appropriée dépend de la nature du risque et des variables situationnelles qui influencent la gamme de choix de l'organisation ; par exemple, financier limitation peut influencer la faisabilité de certaines stratégies telles que l'auto assurance. En développement stratégies de gestion des risques, une organisation devrait utiliser une approche systématique pour identifier, classer et comprendre les risques.

Concernant l'identification des risques, pour (Guye, Leroy, Barr, & Raimbault, 2010), les risques connus sont plus aisément identifiables dans la mesure où l'on possède un ensemble de données sur ces derniers, de plus leur horizon temporel est celui du court terme. Il n'en va pas de même pour les risques émergents (risques nouveaux ou en développement) et futurs, dont les horizons sont le moyen terme et le long terme.

Figure 9: Identification de risques dans le présent et le futur.



Source : (Guye, Leroy, Barr, & Raimbault, 2010).

Dans un tel contexte, et face à la diversité des risques émergents, la gestion des risques se doit d'évoluer, de s'adapter. Comme l'évoque (Guye, Leroy, Barr, & Raimbault, 2010), « le défi est de taille, mais le moment est opportun sans doute pour repositionner ces enjeux de

risques émergents au sein de la stratégie des organisations.

En fin, la gestion des risques vise à assurer que la disponibilité, l'intégrité et la confidentialité des données ne soient pas compromises. Ce sont là les trois principes de la sécurité informatique. On identifie et évalue les risques pour pouvoir les maîtriser, les réduire ou les gérer au mieux.

2.4.4 Analyse des risques SI

Toute décision comporte des risques. Normalement, l'ampleur du risque d'introduction les nouveaux investissements sont positivement liés aux ressources nécessaires. Les risques SI sont positivement liés à dépendre du soutien du SI. (Nosek, 1989) a souligné que les entreprises recherchent des rendements plus élevés, systèmes de risques pour optimiser leur gestion des ressources d'information. À mesure que les organisations deviennent plus dépendantes du SI, la nécessité d'évaluer et gérer les risques devient plus importante.

Selon (McGaughey, Snyder, & Carr, 1994), les organisations doivent évaluer de façon réaliste les risques liés à leurs décisions d'investissement informatique et intégrer la gestion des risques dans la planification du SI et contrôle. Le processus d'évaluation des risques informatiques peut être facilité en employant certains cadres ; l'un d'eux permet une revue systématique de l'investissement informatique dans divers processus ou fonctions organisationnels critiques.

(Porter & Millar, 1985) Suggèrent que les cadres supérieurs suivent cinq étapes pour positionner leur entreprise, afin de profiter de nouvelles opportunités :

- Évaluer l'intensité de l'information en termes de chaîne de valeur et le produit ;
- Déterminer le rôle de l'informatique dans la structure de l'industrie ;
- Identifier et classer les façons dont l'informatique pourrait créer un avantage concurrentiel, l'interne et les liens externes, les composantes du système de valeurs, la portée concurrentielle et les des produits ;
- Découvrez comment l'informatique peut générer de nouvelles activités ;
- Élaborer un plan pour tirer parti des technologies de l'information.

2.4.5 Outils ou techniques pour identifier de nouveaux types de risques

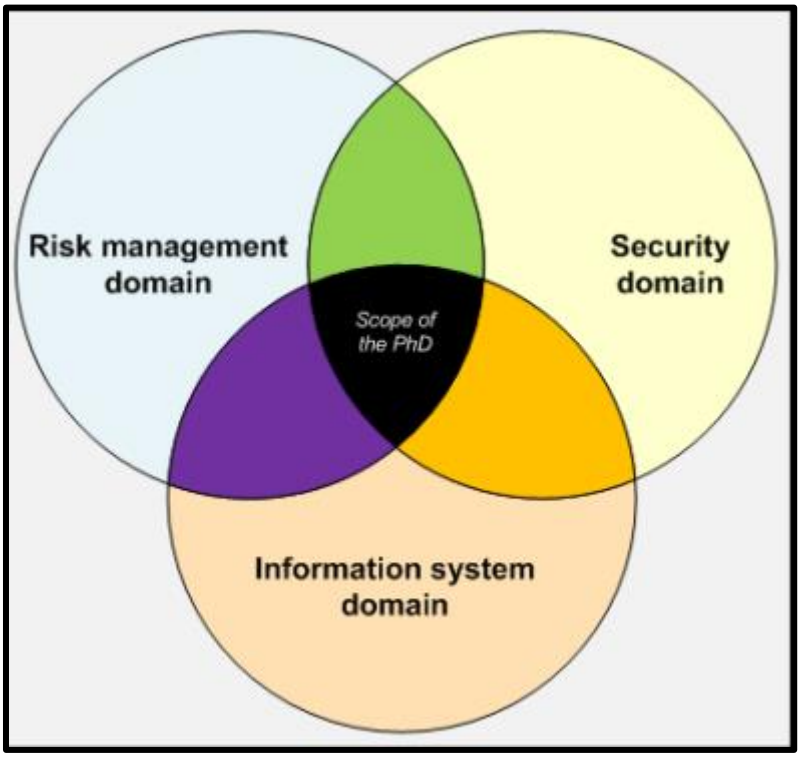
Dans le processus de gestion des risques, la tâche d'analyse des risques vise à identifier et estimer les risques et leurs composantes. De nombreux outils ont déjà été proposés pour une identification et spécification de nouveaux types de risques, menaces ou vulnérabilités.

On peut citer par exemple les arbres d'attaque (attack trees) (Schneier, 2000), utiliser des arbres pour définir précisément les attaques.

Pour la tâche d'analyse des risques, ceux-ci s'appuient sur les bases de connaissances existantes sur les risques/menaces/vulnérabilités. L'utilisateur les utilisera pour choisir les composants les plus pertinents à son contexte.

2.4.6 SI, sécurité et gestion des risques

Figure 10: périmètre lié au domaine gestion des risques, sécurité et SI.



Source : (Porter & Millar, 1985).

2.4.7 Impact gestion des risques SI sur la performance organisationnelle

La performance organisationnelle d'une entreprise dépend de la performance de son SI, elle se manifeste à travers les caractéristiques de ce dernier et la qualité de la circulation de l'information entre les services et entre les niveaux hiérarchiques.

De manière générale, la majorité des directeurs et responsables ont mis l'accent sur la nécessité de performance d'un SI pour avoir un meilleur partage de l'information et la coordination entre les différentes entités de l'entreprise et particulièrement de faciliter la prise de décision ainsi que les orientations stratégiques des directions, ce qui a été confirmé d'ailleurs par (Regragui & Meriouh, 2017).

La relation entre le SI et la performance se manifeste également à travers l'augmentation des résultats financiers (réduction des couts, augmentation de la rentabilité financière) et l'amélioration de la performance commerciale (augmentation du CA, réduction de temps de livraison, augmentation de la production). En effet, l'importance du SI et le considèrent l'une des sources de performance organisationnelle soit d'une façon directe ou indirecte.

De manière générale, le SI reste indispensable dans chaque entreprise, quels que soit sa nature ou son secteur d'activité vu les retombées qu'il engendre sur son activité. Le SI est en relation avec la performance organisationnelle et constitue un levier stratégique, ce qui rejoint les études antérieures réalisées autour de cette thématique.

2.5 ISM

(Qingxiong, Johnston, & Pearson, 2008), dans le cadre de leurs efforts continus pour établir une efficace gestion de la sécurité de l'information (ISM), les chercheurs et les praticiens de la sécurité de l'information ont proposé et développé de nombreuses normes et directives différentes en matière de sécurité de l'information.

Nous avons énormes cas d'utilisation ISM, parmi eux :

- Sécurité d'internet ;
- Cryptage de données ;
- Documents de configuration ;
- Sélection matérielle et logiciels ;
- Intégrité du système (données) ;
- Surveiller et auditer ;
- Gestion de risques…etc.

2.6 ISRM

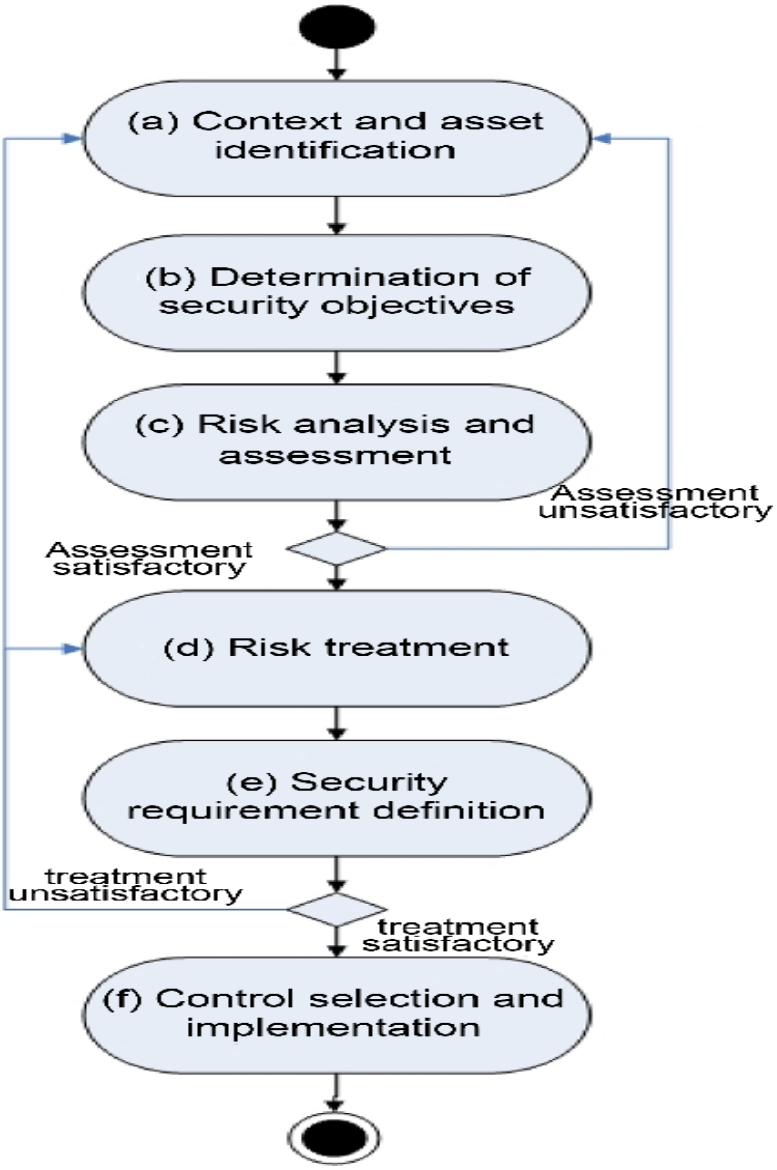
Cette partie s'intéresse à l'introduction d'une stratégie globale de sécurité de l'information-cadre de gestion des risques (ISRM) pour les entreprises utilisant l'informatique. (Saleh & Alfantookh, 2011). Le périmètre structurel du cadre repose sur cinq domaines : stratégie, technologie, organisation, personnes et environnement ; vision qui devient de plus en plus importante pour structurer les questions de sécurité de l'information sur ses domaines distincts. Et le processus de gestion du cadre est associé aux cinq phases du modèle six-sigma bien connu : définir, mesurer, analyser, améliorer et contrôler. De plus, le cadre ajoute des critères de gestion à ses enjeux structurels ; et envisage des outils d'évaluation pour ses

phases procédurales.

2.6.1 Introduction au processus ISSRM

Les activités ISSRM suivent généralement un processus global composé d'étapes classiques généralement trouvées dans les méthodes ISSRM traditionnelles. Néanmoins, on doit noter que les différentes méthodes ne mettent pas le même poids sur les activités exercées et c'est l'une des principales particularités de chaque méthode/norme. Certaines méthodes, par exemple, sont davantage axées sur l'évaluation des risques. Tandis que d'autres suggèrent d'appliquer des contrôles de sécurité standard (ou des contre-mesures) afin d'atteindre un niveau de sécurité. L'ensemble du processus ISSRM est résumé dans la (figure 09).

Figure 11: processus ISSRM.



Source : (Saleh & Alfantookh, 2011).

Pour le processus ISSRM présenté dans la figure 09, il se compose de six étapes à savoir :

- **Identification du contexte et des actifs** :
  Le processus commence par une étude du contexte de l'organisation et l'identification de ses atouts. Dans cette étape, l'organisation et son environnement sont décrits, en mettant l'accent sur les activités sensibles liées à la sécurité de l'information. Une vue d'ensemble du SI, quand déjà en place, est faite.
- **Détermination des objectifs de sécurité :**
  Les besoins de sécurité de l'organisation sont alors définis. Sur la base de l'identification des actifs, il faut déterminer les objectifs de sécurité à atteindre. Les objectifs de sécurité sont souvent définis en termes de propriétés de confidentialité, d'intégrité et de disponibilité des atouts.
- **Analyse et évaluation des risques :**
  L'étape principale du processus est l'analyse des risques, en identifiant les risques qui menaçant les objectifs de sécurité. Cette étape consiste à identifier les risques et à estimer leur niveau de manière qualitative ou quantitative.
- **Traitement des risques :**
  Une fois l'évaluation des risques effectuée, des décisions concernant le traitement des risques sont pris. Risque les mesures de traitement peuvent comprendre l'évitement, la réduction, le transfert ou le maintien du risque :
    - ✓ L'évitement des risques est la décision de ne pas s'impliquer ou l'action de se retirer d'une situation à risque. Par exemple, n'utilisez pas la fonctionnalité risquée du SI et donc désactivez le risque ;
    - ✓ La réduction des risques consiste à prendre des mesures pour réduire la probabilité, les conséquences négatives, ou les deux, associées à un risque. Par exemple, sélectionnez et implémentez une sécurité exigences pour atténuer le risque ;
    - ✓ Le transfert de risque consiste à partager avec une autre partie la charge de la perte d'un risque. Par exemple, prendre une assurance pour couvrir les conséquences du risque ;
    - ✓ La rétention des risques est l'acceptation du fardeau de la perte d'un risque particulier, par exemple, accepter le risque tel quel parce que sa probabilité et ses conséquences sont suffisamment faibles.

- **Définition des exigences de sécurité :**
  Les exigences de sécurité sur le SI peuvent ainsi être déterminées comme des solutions de sécurité pour atténuer les risques, principalement si le traitement de réduction des risques a été choisi. Cependant, des exigences de sécurité peuvent émerger d'autres traitements, comme le transfert de risques nécessitant généralement certaines exigences vis-à-vis du tiers.
- **Sélection et mise en œuvre des contrôles :**
  Les exigences sont finalement instanciées dans des contrôles de sécurité, c'est-à-dire des contre-mesures spécifiques au système, qui sont mises en œuvre au sein de l'organisation. Exemple : Un pare-feu et un système de détection d'intrusion (IDS) sont sélectionnés et mis en œuvre au sein du SI.

2.6.2 Exigences de sécurité et gestion des risques

L'application de toute approche ISRM a généralement trois résultats principaux (Stoneburner, Goguen, & Feringa, Risk Management Guide for, 2002) :

- L’amélioration de la sécurité du SI ;
- La justification du budget et de l'investissement pour les décisions de gestion de la sécurité du SI ;
- L'évaluation du niveau de confiance que les clients ou partenaires peuvent avoir dans le SI.

Par conséquent, le premier avantage de l'ISRM est qu'il permet de traiter les trois principaux acteurs concernés par la sécurité du SI : développeurs SI, responsables d'organisation et clients de l'organisme. Il fournit pour chacun d'eux des résultats au niveau de leurs préoccupations, c'est-à-dire, niveau technique, niveau financier et niveau de confiance du SI.

2.6.3 Normes de gestion des risques

Les référentiels de gestion des risques sont des référentiels de haut niveau présentant la gestion des risques en général et Approches de gestion des risques spécifiques au domaine. Dans cette partie nous allons présenter deux normes de gestion des risques des SI, à savoir :

- **ISO/CEI Guide 73 :** (MAYER, 2009)
  L’objectif de Guide ISO/73 est de fournir une base terminologique et des définitions génériques pour la gestion des risques, afin de développer une compréhension commune entre les organisations de tous les pays et entre les

membres de l'ISO et de la CEI (Commission Electronique Internationale).
Le guide est axé sur la gestion des risques en général, quel que soit le domaine concerné. C'est de même applicable aux risques en finance, environnement, gestion de projet, sécurité de l'information risque, etc.
Cette guide est notamment utilisée comme entrée pour la définition ou la révision des autres ISO standard traitant de RM dans un domaine spécifique. Cependant, selon le Guide, il peut être parfois nécessaire de s'écarter de la formulation exacte proposée dans le Guide pour répondre aux besoins d'un domaine spécifique.
Le cœur de la norme ISO/CEI Guide 73 est une liste de définitions sur les concepts de gestion des risques y compris les tâches gestion des risques.

- **AS/NZS 4360 :** (MAYER, 2009)
  AS/NZS 4360 est une norme conjointe australienne/néo-zélandaise. Sa version actuelle date de 2004 et la première a été publiée en 1999.
  Cette norme est intitulée « La gestion des risques » et son objectif est de fournir un cadre générique pour établir le contexte, l'identification, l'analyse, l'évaluation, le traitement, le suivi et la communication des risques.
  Comme pour l'ISO/CEI Guide 73, cette norme est générique et peut être appliqué à tout domaine gestion des risques, ainsi qu'à tout secteur ou organisation.
  AS/NZS 4360 fournit le processus itératif suivant :
    - ✓ Établir le contexte :
      - Définition du contexte (interne et externe) de l'organisation ;
      - Définition des critères par rapport auxquels le risque sera évalué ;
      - Définir la structure pour le reste du processus.
    - ✓ Identifier les risques :
      - Identifier les sources de risques et d'événements qui pourraient avoir un impact sur l'organisation ;
      - Identifier comment ils peuvent se produire.
    - ✓ Analyser les risques :
      - Évaluer les contrôles de sécurité existants qui minimisent déjà les risques ;
      - Estimer l'ampleur des conséquences et la probabilité de l'événement des risques.
    - ✓ Évaluer les risques :

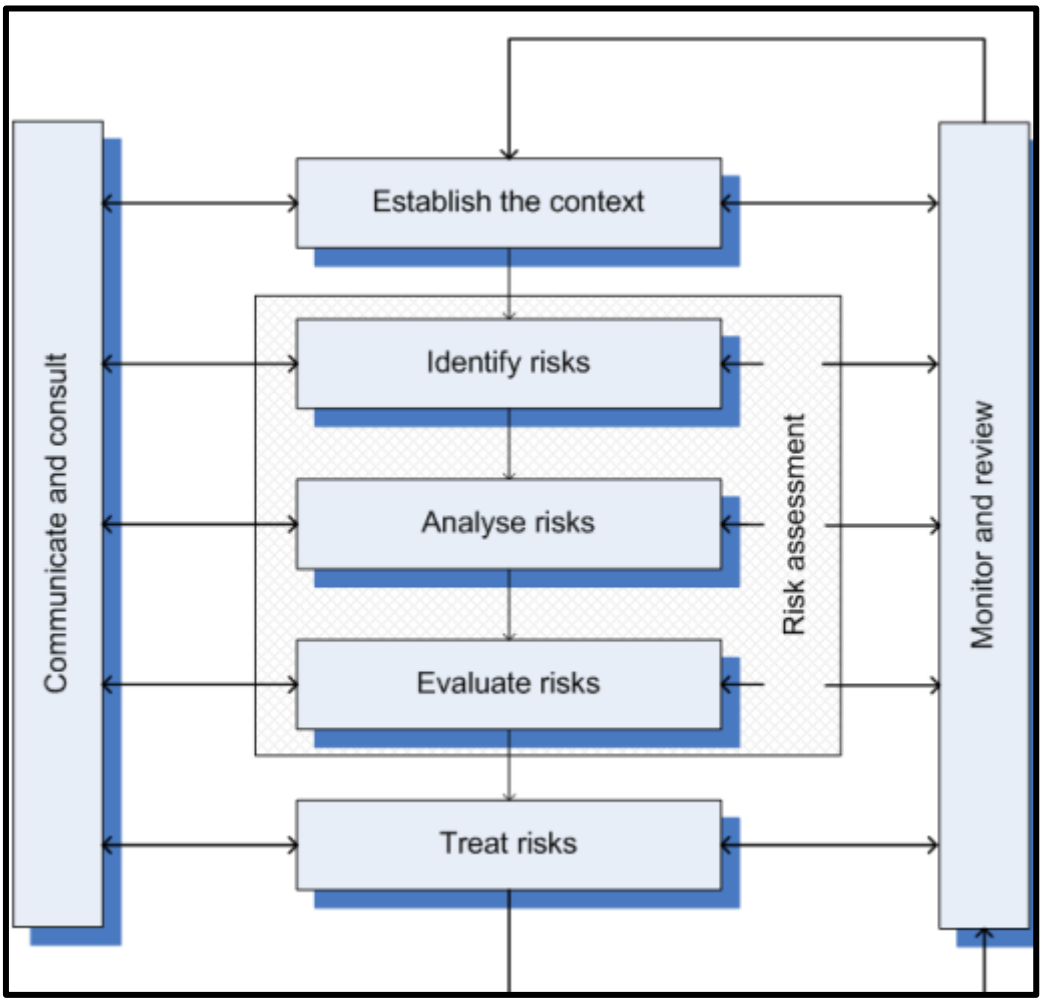
- Prendre des décisions concernant les risques, sur la base des résultats de l'analyse des risques.

✓ Traiter les risques :

- Identifier les options de traitement des risques (ayant des conséquences positives ou négatives) ;
- Sélectionnez l'option la plus appropriée, en équilibrant les coûts de mise en œuvre contre avantages obtenus ;
- Définir et mettre en œuvre un plan de traitement.

La norme se termine par des recommandations pour établir une efficace gestion de risques.

Figure 12: présentation du processus gestion des risques.



Source : (MAYER, 2009).

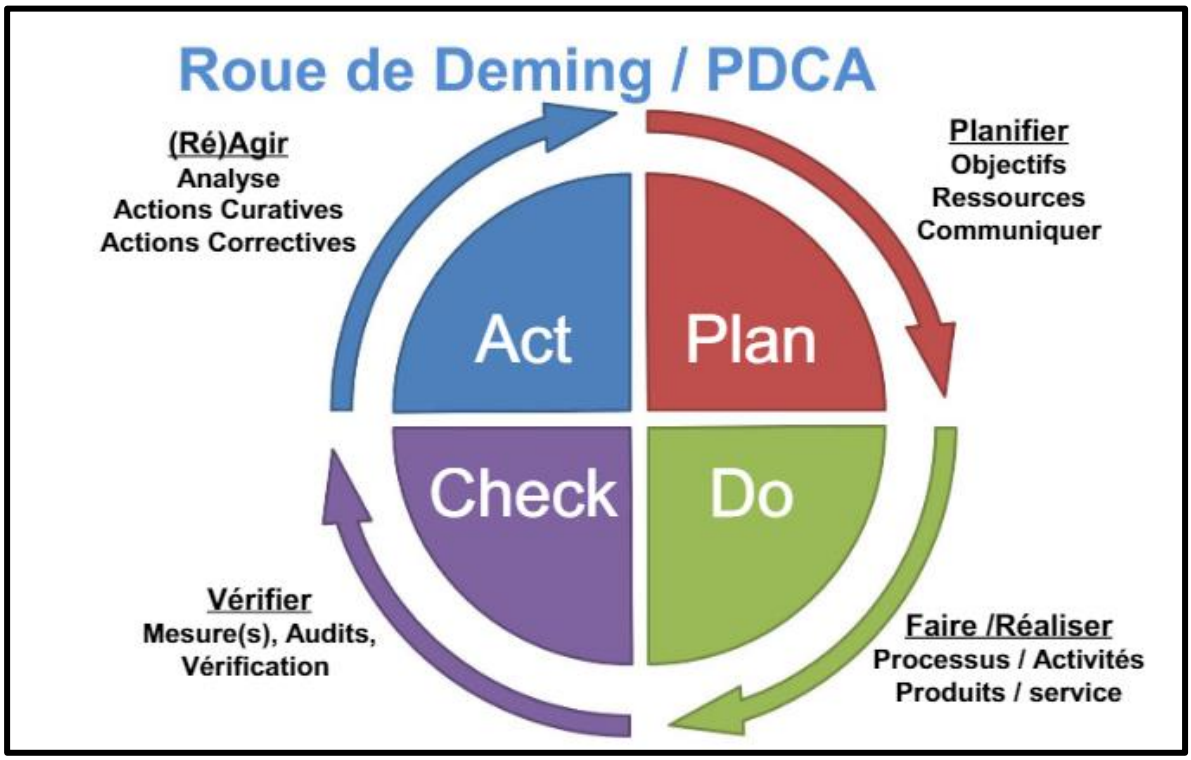
2.6.4 Normes de gestion des risques de sécurité

Cette partie présente les normes traitantes de la sécurité qui sont spécifiquement axées sur

Activités gestion de risques.

- **Série de norme d'ISO/IEC 2700x :** (MAYER, 2009)
  La série de normes ISO/IEC 2700x traite de la gestion de la sécurité de l'information. Elle est composée d'un ensemble de normes fournissant des informations pour la mise en place d'un Système de gestion de la sécurité (ISMS : Information Security Management System).
  Un système de management est défini comme le cadre des processus et des procédures utilisées s'assurer qu'une organisation peut accomplir toutes les tâches requises pour atteindre ses objectifs. Dans le cadre des principes communs partagés par les systèmes de management, la principale est l'application du paradigme Plan-Do-Check-Act (cycle PDCA). Ce cycle est composé des quatre étapes suivantes à effectuer itérativement :
    - ✓ **Plan :** établir les objectifs et les processus nécessaires pour obtenir des résultats conformément avec les spécifications ;
    - ✓ **Do :** mettre en œuvre les processus ;
    - ✓ **Check :** surveiller et évaluer les processus et les résultats par rapport aux objectifs et aux spécifications ;
    - ✓ **Act :** appliquer les actions au résultat pour les améliorations nécessaires.

Figure 13: Roue de Deming PDCA.



Source : certification-QSE.com.

- **ISO/IEC 13335-1:**

  Cette norme est la première de la série de lignes directrices ISO/CEI 13335 qui traite de la planification, de la gestion et de la mise en œuvre de sécurité informatique. Il décrit les concepts et les principes de la sécurité informatique qui peuvent être applicables à différentes organisations (ISO/IEC 27001, 2013).

- **Common Criteria:**

  Standardisé en version 2.3 par ISO/IEC 15408, fournit un ensemble commun d'exigences sur les fonctions de sécurité des produits et systèmes informatiques, et sur les mesures d'assurance qui leur sont appliquées pendant une évaluation de sécurité. La première partie, intitulée « Introduction et modèle général », est la plus pertinente par rapport à notre champ de recherche (Stoneburner, Goguen, & Feringa, Risk Management Guide for, 2002).

- **NIST 800-27 Rev A [09] /NIST 800-30 :**

  Parmi la série de publications proposée par le NIST, la série 800 concerne la

sécurité informatique. Dans cette série, NIST 800-27 et NIST 800-30 sont dans notre champ d'application. La terminologie et les concepts sont fournis par ces normes, qui sont cohérentes entre elles.

2.6.5 Dimension ISRM dans une organisation

Le cadre cible de l'approche ISRM comporte deux parties principales : une partie concerne sa vue structurelle ; tandis que l'autre est associée à sa vue procédurale.

La vue structurelle a deux dimensions : portée et critères ; tandis que le point de vue procédural a deux autres dimensions : le processus et les outils.

Du coup, les quatre dimensions d'ISRM sont : (Saleh & Alfantookh, 2011)

1. **Portée :** est basées sur les cinq domaines, à savoir stratégie, technologie, organisation, personne, et l'environnement avec différents niveaux de détails, associés à chaque domaine.
2. **Critères :** est considérée comme associé avec les contrôles de la famille ISO de normes de sécurité de l'information. Cependant, d'autres exigences peuvent également être envisagées.
3. **Processus :** adopte les cinq phases cycliques du modèle six sigma, qui sont définir, mesurer, analyser, améliorer et contrôler.
4. **Outils :** peut inclure les divers moyens qui ferait la promotion du travail, y compris : des outils d'enquête, des modèles mathématiques et logiciel.

2.7 Enjeux de la sécurité de l'information pour les organisations

L'information est aujourd'hui unanimement considérée comme un actif stratégique pour l'entreprise. En même temps, il s'agit d'un actif intangible, dont la valeur est difficilement mesurable et dont la prise de conscience pourrait être amplifiée chez les dirigeants.

Pour (CIGREF, 2008), il a classé les risques liés aux usages IT au sein d'une entreprise de différentes façons, par exemple :

- Risques informationnels ;
- Risques liés aux applications ;
- Risques liés aux développements ;
- Risques liés à la maintenance ;
- Risques liés aux infrastructures, serveurs ;

- Risques liés aux projets ;
- Risques liés aux fournisseurs.

CHAPITRE Ⅱ : CADRE MÉTHODOLOGIQU ET ORGANISATIONNEL

Section 1: Cadre méthodologique

Après avoir entamé une partie théorique, composée de revue de littérature et cadre conceptuel, nous allons essayer à travers ce chapitre d'exposer l'approche épistémologique, ensuite nous présenterons la méthodologie utilisée dans notre travail de recherche sur la gestion des risques d'un système d'information.

1.1 Posture épistémologique

L'épistémologie est l'étude des théories et les principes de la connaissance. C'est un nouveau concept, qui a apparu aux débuts du 20èm^{e} siècle. Et nous extrairons plusieurs définitions, à savoir :

"L'épistémologie est la théorie de la connaissance. Dans nos investigations épistémologiques, nous réfléchissons sur les critères auxquels une connaissance véritable devrait se conformer" (HARRE, 1984).

"L'épistémologie est la partie de la philosophie des sciences qui considère la manière dont les savoirs s'organisent" (FOUREZ, 1988).

"Ce mot désigne la philosophie des sciences, mais avec un sens plus précis. (...) C'est essentiellement l'étude critique des principes, des hypothèses et des résultats des diverses sciences, destinée à déterminer leur origine logique (non psychologique), leur valeur et leur portée objective." (LALANDE, 1991).

À travers la revue de la littérature et le cadre conceptuel, nous nous sommes aperçus de l'importance de la question de recherche dans le monde de l'entreprise et qui nous a menés à adopter un paradigme positiviste.

1.2 Approche méthodologique

Nous visons dans ce travail à restituer un positionnement qui s'est nourri d'une double appartenance communautaire, le contrôle de gestion et le management de la sécurité des SI. À l'intersection de ces disciplines, nous avons opté pour une méthodologie d'enquête qualitative afin de mésuser la qualité de sécurité des SI.

Cette étude qualitative a pour but de comprendre ou expliquer le phénomène du management de sécurité des SI. Il s'agit d'une méthode de recherche plus descriptive et se concentre sur des interprétations, des rapports de tests de sécurité et leurs significations.

Là où la tradition quantitative cherche souvent à éliminer la subjectivité dans les données analyser l'influence de facteurs extérieurs aux individus sur leurs actions, de leur côté, les méthodes qualitatives abordent directement la subjectivité des acteurs et comprennent de manière approfondie.

Dans notre cas de recherche et après l'identification de tout ce qui a de l'importance aux yeux des acteurs et estimer d'avoir compris comment tous ces éléments s'entremêlent et fonctionnent conjointement. Le but des méthodes qualitatives est de faire le tour du problème, c'est-à-dire épuiser le stock de variables pertinentes et « dessiner » le système qu'elles composent ensemble.

Ensuite, notons que si elle est bien conduite, notre analyse qualitative prend en compte le caractère multifactoriel du SI étudié, puisqu'elle s'attache par définition à identifier l'ensemble des variables pertinentes à la compression du phénomène de management des risques.

Cependant, comme le souligne précisément (Piguet, 2010), ils ne peuvent donner des estimations chiffrées du phénomène. La méthode qualitative ne permet pas ainsi que mesurer l'interdépendance entre différents facteurs, et ainsi voir les relations les plus précises et les moins importantes.

1.3 Méthodes de collecte des données

La collecte de données est un élément crucial du processus de recherche en management, elle constitue un moyen sur lequel le chercheur fond sa recherche. En effet, quel que soit le type d'évaluation menée, il est essentiel de bien choisir les méthodes de collecte et d'analyse des données et de les appliquer correctement.

Nous avons commencé la planification de la collecte de données en examinant dans quelle mesure il est possible d'utiliser les données existantes. Concernant notre cas il s'agit de récupérer les statistiques et les résultats des rapports de sécurité du SI étudié.

Pour mener une étude empirique, nous avons eu recours à plusieurs techniques à la fois. D'abord, nous avons mené une observation pour faire émerger de nouvelles hypothèses ou des pistes de travail qui nous ont poussés à réaliser une étude de cas pour comprendre le management de la sécurité des systèmes d'information.

Dans notre cas d'étude, étude qualitative, et grâce à plusieurs techniques d'enquête, l'étude

qualitative permet de collecter des données informatives :

1.3.1 Entretien

La technique de l'entretien est très utile dans la collecte de données informatives sur des sujets très précis. Il s'agit surtout de s'entretenir avec des personnes qui ont une expertise ou une expérience particulière sur votre sujet.

Les différents types d'entretiens (directif, semi-directif ou libre) permettent de récolter des informations à travers une discussion avec une ou plusieurs personnes.

1.3.2 Observation

La technique de l'observation s'avère utile quand le chercheur étudie un phénomène, un sujet, réel, qui est observable.

Que l'observation soit participante, non participante, structurée ou non structurée, elle permet de collecter des données intéressantes.

1.3.3 Groupe de discussion

Le groupe de discussion (qu'il soit homogène ou hétérogène) permet au chercheur de faire interagir plusieurs personnes, afin de collecter des informations en faisant émerger diverses opinions grâce aux débats.

À l'instar de l'entretien ou de l'observation, le groupe de discussion permet de collecter des données émanant de plusieurs personnes, parfois en désaccords.

Le groupe de discussion peut être utile lorsque le sujet et son interprétation dépendent de la situation sociale d'un groupe de personnes, ou s'il s'agit d'un sujet de société.

1.3.4 Recherche documentaire

Afin d'enrichir notre mémoire, nous avons :

- Sélectionné les sources d'information ;
- Cherché et localisé les documents ;
- Evalué la qualité et la pertinence des sources ;
- Met en place une veille documentaire.

1.3.5 Etude de cas

Les études de cas permettent d'analyser en profondeur les phénomènes dans leur contexte,

ce qui est sa plus grande force. Cependant, l'utilisation de cette méthode qualitative est soumise à des normes scientifiques et doit être soumise à un degré de rigueur au moins équivalent à celui des méthodes de recherche quantitatives, (Yves-C, 2012).

La réalisation de cette méthode de recherche requis sept étapes, à savoir :

- **Etablir la pertinence :**
  - Définir l'approche à laquelle nous adhérons ;
  - Circonscrire sommairement la problématique de recherche ;
  - Répondre à certaines questions pour établir la pertinence.
- **Assurer la véracité des résultats :**
  - Utiliser des descripteurs concrets et précis ;
  - Protéger les données brutes ;
  - Recourir à de multiples chercheurs pour réaliser la recherche ;
  - Confirmer les données recueillies auprès d'informateurs ;
  - Faire réviser l'interprétation des données par des pairs.
- **Développer le cadre de recherche :**
  - Développer la question de recherche ;
  - Choisir entre l'étude d'un cas unique ou multiple ;
  - Choisir la technique centrale et les sources potentielles de collecte des données ;
  - Identifier la population cible et établir les critères de sélection des cas ;
  - Se familiariser avec le phénomène à étudier.
- **Déposer d'un nombre de suffisant cas caractéristique pour réaliser la recherche :**
  - Acquérir une bonne connaissance de la dynamique du milieu ;
  - Vérifier s'il y a des relations professionnelles autres que celle liées à la recherche ;
  - Surveiller la répartition géographique des cas ;
  - Recruter plus de cas que le nombre requis.
- **Collecte de données :**
  - Se faire accepter dans les milieux observés ;
  - Pratiquer l'observation et l'écoute active ;
  - Recourir au plus nombre de sources d'information ;

- Gérer les données recueillies ;
- Assurer un retrait en douceur du terrain d'étude.

- **Traitement des données :**
  - Epurer les données recueillies ;
  - Codifier les données recueillies ;
  - Analyser les données codifiées ;
  - Rédiger chaque étude de cas.
- **Diffuser les résultats :**
  - Choisir le type de diffusion ;
  - Cerner les exigences du média et les caractéristiques de l'audience visée ;
  - Rédiger le contenu de la diffusion.

De plus, dans notre étude de cas, nous passons en revue toutes les théories existantes sur la gestion de la sécurité des systèmes d'information, et à cet égard, nous bénéficions de la vaste collection d'ouvrages, de mémoires et d'articles de la bibliothèque de l'école E.N.S.M.

1.4 Méthode d'analyse

Méthode d'analyse peut aider à mesurer la performance organisationnelle, basée sur la méthodologie de l'analyse de management, et qui peut nous donne des résultats et des graphes d'une vision générale de la gestion des SI dans les entreprises.

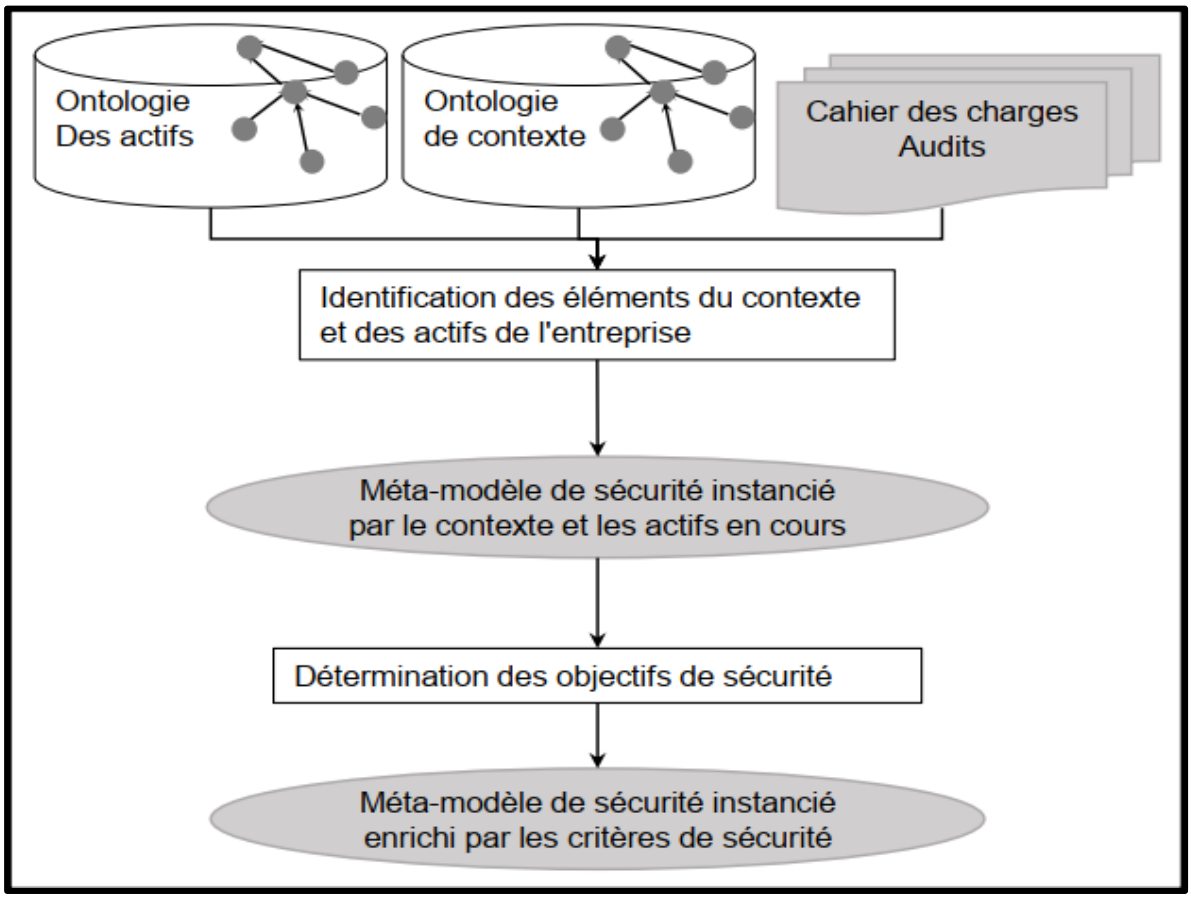
L'objectif de notre recherche est de décrire, de comprendre la stratégie de management de la sécurité du SI dans les entreprises, et cela se fait par l'analyse des données collectées.

Pour pouvoir arriver à la réalisation de cette analyse, nous avons passé par toute une étude de gestion de SI et plus particulièrement le processus gestion des risques, chose qu'il parait difficile en premier lieu à cause d'une grande difficulté d'avoir des informations d'une façon directe et facile ce qui nous a obligés de faire une étude de cas. Afin d'avoir une vision générale de l'état de sécurité de l'organisation.

1.5 Processus d'enrichissement du méta modèle de la sécurité

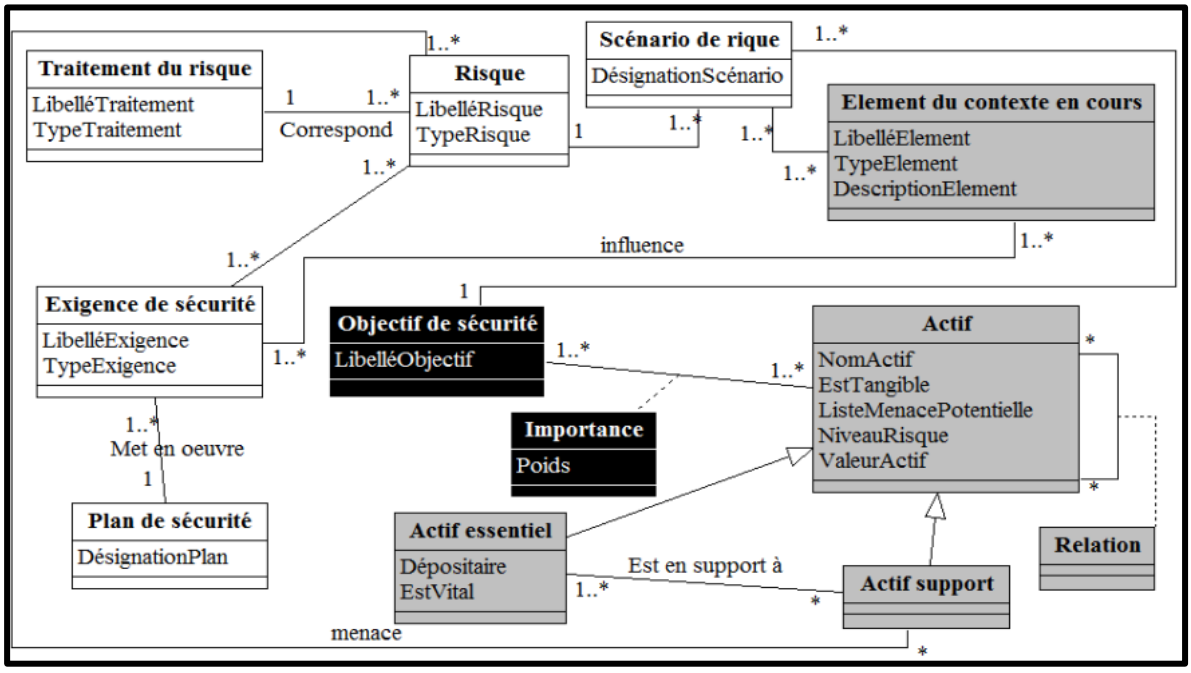
Nous présentons dans la figure ci-dessous une démarche en deux phases qui permet d'instancier le méta modèle de sécurité (Figure 15) qui sert de base au processus de dérivation des objectifs de sécurité fondée sur l'analyse des risques.

Figure 14: Processus d'enrichissement du méta modèle de la sécurité.



Source : (Akoka, Laoufi, & Lammari, 2018).

Figure 15: Méta modèle de la sécurité.



Source : (Akoka, Laoufi, & Lammari, 2018).

Notre méta modèle a été construit sur la base de nos travaux antérieurs (Akoka, Laoufi, & Lammari, 2018). Il est composé de trois groupes de concepts. Le premier groupe (en noir) est constitué des concepts relatifs aux objectifs de sécurité. Le second groupe (en blanc) est relatif aux concepts utilisés dans la phase de dérivation des exigences de sécurité. Le dernier groupe (en gris) est composé des concepts relatifs au contexte qui comporte aussi ceux des actifs. Les vulnérabilités sont des propriétés de ces derniers. Toutefois, il faut noter que les vulnérabilités sont une des composantes du risque. Il y a une relation entre le concept de risque et le concept d'actif support qu'on dénomme menace. Les critères de sécurité sont proposés pour les actifs de l'organisation, comme le propose le modèle des actifs de la méthode ISSRM. Chaque relation possède un poids défini d'après la situation d'exploitation de l'actif. Cette valeur est tirée des méthodes utilisées généralement pour la construction de l'ontologie des actifs (Akoka, Laoufi, & Lammari, 2018). Nous considérons que les actifs font partie du contexte. L'ensemble des actifs sont inclus dans l'ensemble du contexte, si tous les éléments des actifs sont aussi éléments du contexte.

Section 2: Cadre organisationnel

2.1 Contexte de cas pratique

2.1.1 Choix du sujet

Choisir un sujet pour votre mémoire n'est pas une chose facile. Il est extrêmement important de choisir un sujet de mémoire actuel et pertinent. En effet nous avons opté pour le thème **management des risques de systèmes d'information**. Le choix du sujet est argumenté comme suit :

- Un sujet en lien avec ma formation master management e-gouvernement ;
- Un sujet qui m'intéresse, qui j'aurais plaisir à approfondir ;
- Un sujet de mémoire actuel et utile ;
- L'existence d'assez de sources scientifiques sur ce sujet d'étude.

2.1.2 Choix de lieu stage

- **Pourquoi choisir CR METAL/ENCC ?**

  CR METAL/ENCC est une unité phare et complète de l'Entreprise Nationale de charpente et de chaudronnerie. En effet un SI adéquat qui peut nous accompagner dans la réalisation de notre recherche dans toutes ses étapes :

  - Confirmation de la sélection du sujet ;
  - Formulation de la problématique et des hypothèses ;
  - Recueil des données ;
  - Sélection de la méthode de recherche ;
  - Rédaction et finition de mémoire de recherche.

2.1.3 Difficultés apportées

Les principales contraintes que nous avons côtoyées dans notre aventure durant le stage ou rédactionnel :

- Trouver un bon stage ;
- Construction d'un bilan général de notre recherche ;
- Se forcer à s'y remettre.

2.2 Présentation de l'organisation d'accueil

2.2.1 Présentation du CR METAL/ENCC

- **Renseignement :**

Le leader algérien dans le domaine de la construction métallique et la chaudronnerie.

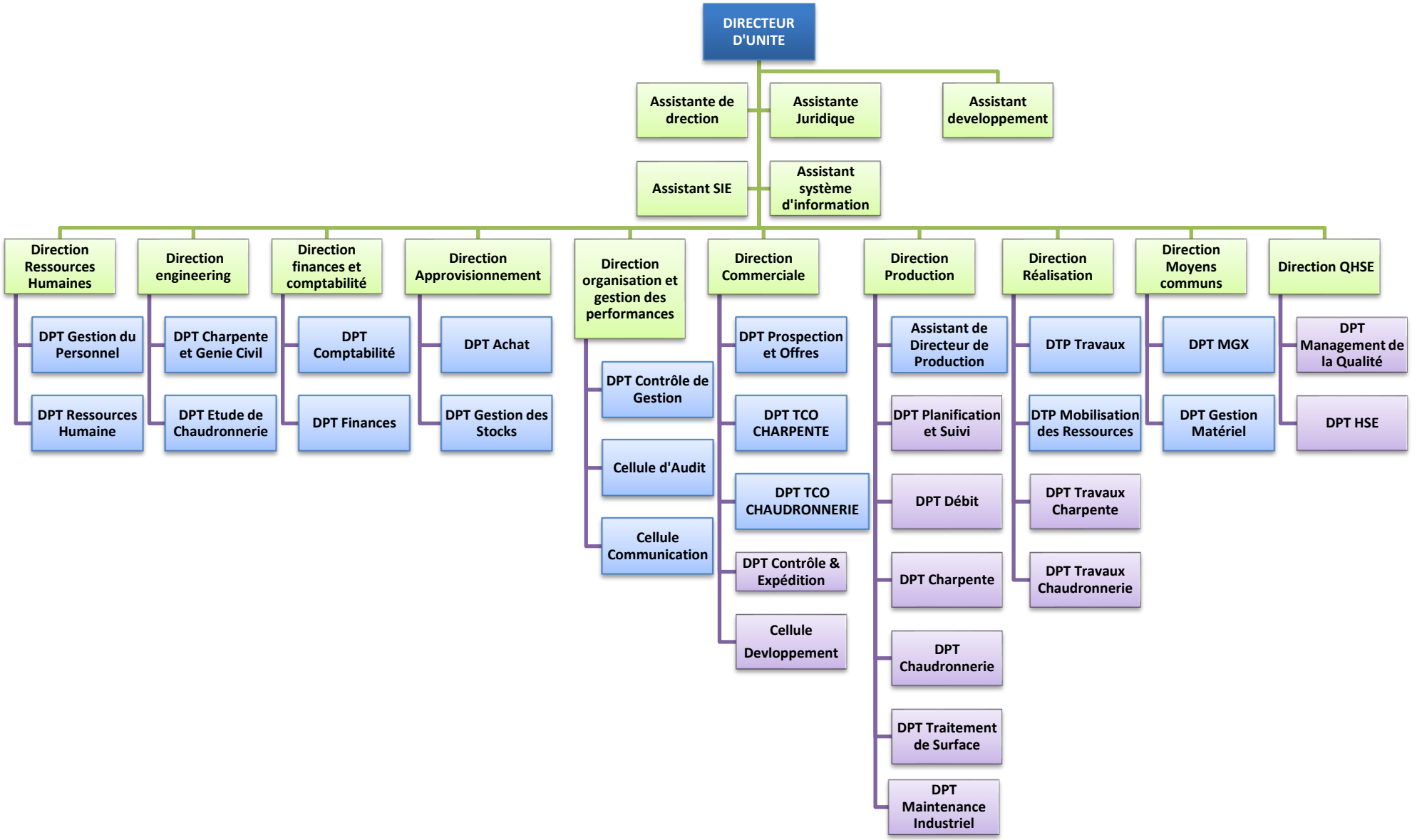
Address: 130 Avenue Kritli Mokhtar BP n° 01., Blida, Algeria.

Site : encc-crmetal.dz.

Contact : 025.30.53.59.

- **Activités de CR METAL/ENCC**
  - Maintenance et rénovation : Rénovation des installations Oil & Gas, maintenance des équipements industriels ;
  - Montage industriel : Montage des bacs, montage de la charpente métallique ;
  - Fonds bombés : Fonds bombés elliptiques, Fonds plats, Calottes sphériques ;
  - Charpente métallique : Simples et technologiques, y compris couverture, bardage, serrureries, électricité, climatisation, etc.
  - Chaudronnerie : Cuves standards, GPL-c, Bacs de stockage jusqu'à 50 000 M3 ;
  - Equipements industriels : Conteneurs, Bac à eau, Bac à boue, Circuit à boue, Bac de jaugeage, Séparateurs à gaz, Station mobile pour carburant et Kérosène.

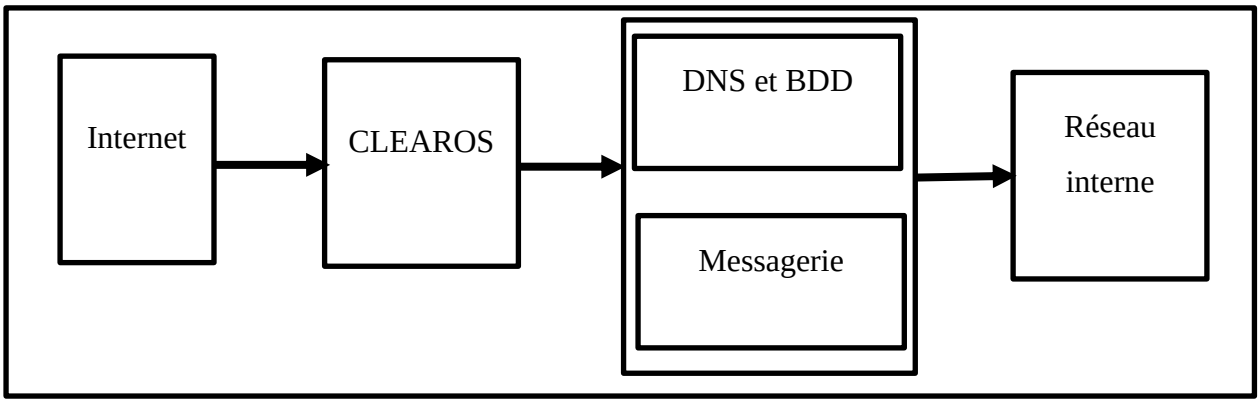
2.2.2 Organigramme du CR METAL/ENCC



2.2.3 Système d'information du CR METAL/ENCC

- **Schéma réseau informatique général du CR METAL**

Figure 16: schéma réseau générale



Source : documentation CR METAL.

- **Description du réseau de la CR METAL**

  Dans la présente partie, nous allons présenter le réseau informatique dans la CR METAL, ainsi nous présentons la méthode de sécurité adoptée par l'entreprise pour la protéger de tous les risques d'attaques ou d'intrusions. Ces intrusions consistent généralement pour les hackers à exploiter les failles du réseau ou d'une application ou bien encore une mauvaise gestion des comptes utilisateurs.

  - **Modèle réseaux faste Ethernet 1/100 :**

    La norme faste Ethernet (IEEE 802.3u) a été établie. Cette norme pose la limite de vitesse Ethernet de 10 à 100 Mbps.

  - **Câblage :**

    Cable à paires torsadées, câble à paire torsadée droit et connecteur RJ45.

  - **Serveur BDD:**

    Intel core i5-540 processor, 4GB of DDR3.

  - **Switch 24 port D-LINK:**

  - **Serveur DNS :**

    Le protocole DNS est utilisé de manière transparente pour effectuer la correspondance entre un nom de machine compréhensible et son adresse IP.

  - **Serveur messagerie VPOP3:**

- Est un serveur pleinement fonctionnel email Windows ;
- VPOP3 peut détecter plus de 80% des spams, il peut également détecter et bloquer les virus e-mail automatiquement à l'aide d'Avast (antivirus).

- **Serveur firewall (CLEAROS) :**

Le serveur firewall permettant de protéger un ordinateur ou un réseau d'appareils des intrusions provenant d'un réseau tiers (notamment internet).

Le serveur pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivantes :

- Une interface pour le réseau à protéger (réseau interne) ;
- Une interface pour le réseau externe.

CHAPITRE Ⅲ : ÉVALUATION DU SYSTÈME D'INFORMATION

On va essayer durant ce chapitre pratique, d'appliquer les principaux sujets retenus dans les deux chapitres qui précédent pour arriver enfin à trouver une réponse à la problématique principale de ce travail de recherche. Pour cela, on a choisi l'entreprise CR Métal/ENCC comme organisation de recherche.

La sécurisation de SI du CR METAL est basée sur des applications et équipements bien précis, à savoir :

- **Kaspersky Security center 11 (Version 11.0.0.1131) :** est une console d'administration unique qui permet la sécurité et la gestion des systèmes informatiques, aussi contrôler les outils de sécurité et d'administration système. Kaspersky est installé à CR METAL en tant que console Web.
- **Serveur Firewall (pare-feu) :** est un outil informatique (matériel et/ou logiciel) conçu pour protéger les données d'un réseau. Dans le cas du CR METAL protection de réseau de l'entreprise ou protection d'un ordinateur relié à l'internet par le Firewall CLEAROS présenté dans la (figure 16).
- **Protection des postes de travail :**
    - Protection des mots de passes ;
    - L'accès à, l'Internet se fait à partir d'un serveur sécurisé ;
    - Soumettre tous mail et tout document téléchargé à une détection des virus et code malicieux ;
    - Activer et mettre à jour un programme de protection complet ;
    - Un dossier partagé sur le contrôleur de domaine**.**

En effet, la sécurisation du SI de CR METAL assure les critères fondamentaux de la sécurité de l'information, ces critères concernent des caractéristiques que le propriétaire ou le gestionnaire de l'information veut voir réaliser afin d'assurer la sécurité. Nous avons : la **confidentialité**, l'**intégrité**, la **disponibilité**, la **traçabilité** et l'**Authenticité.**

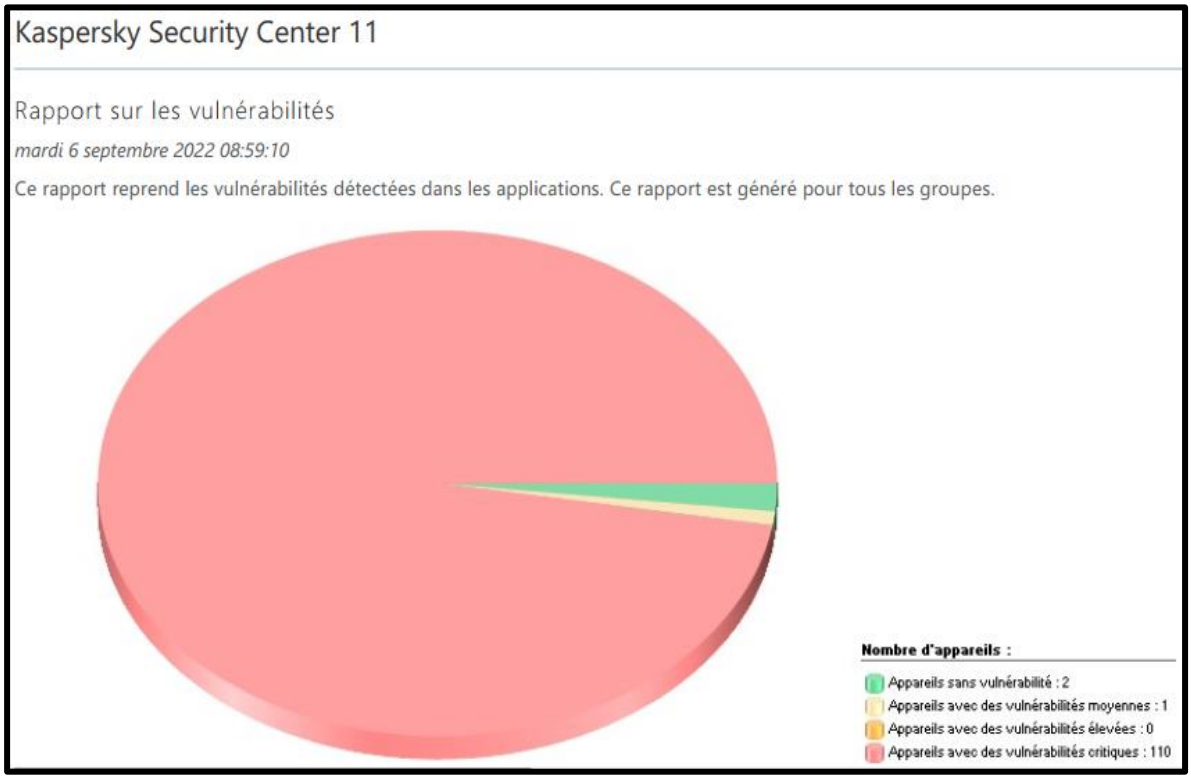
Section 1: Interprétation et discussion des résultats obtenus

Cette section porte sur le processus d'interprétation des résultats en recherche qualitative et vise à fournir des réflexions théoriques et des conseils pratiques. Afin de nous permettre de répondre de notre problématique et de suggérer des solutions pratiques.

À travers Kaspersky sécurité center installé sur les différents appareils du SI de CR METAL, et qui est chargé au niveau de l'organisation de la sécurité informatique. Nous obtenions les rapports suivants :

1.1 Rapport sur les vulnérabilités

Figure 17: diagramme circulaire présente les degrés de vulnérabilités.



Source : assistant SI CR METAL.

D'après le rapport de 06 septembre 2022, qui reprend les vulnérabilités détectées dans les applications :

- 02 appareils sans vulnérabilité ;

- 01 appareil avec des vulnérabilités moyennes ;
- 00 appareil avec des vulnérabilités élevées ;
- 110 appareils avec des vulnérabilités critiques.

D'après la figure ci-dessus, nous avons pu extraire les vulnérabilités et leur niveau de criticité. Prenant les vulnérabilités critiques du SI de CR METAL sont les vulnérabilités qui ont relation avec :

Tableau 1: les vulnérabilités critiques.

Editeur	Application	Version installée	Nombre d'appareils
Adobe system	Adobe Reader 6	10.0.1	68
Mozilla Fondation	Mozilla Firefox	19.0	11
Microsoft	Windows 7	/	19
Google	Google Chrome	17.0.963.56	12

Source : élaboré par nous-mêmes.

Les vulnérabilités précédemment identifiées exposent les biens à des menaces. Du coup nous sommes dans l'obligation d'identifier les principales menaces auxquelles notre SI peut être confronté :

- L'utilisateur du système est généralement insouciant, il n'a pas le désir de porter atteinte à l'intégrité de données sur lequel il travaille ;
- une personne malveillante parvient à s'introduire sur le système, légitimement ou non, et à accéder ensuite à des données ou à des programmes auxquels elle n'est pas censée avoir accès ;
- Un programme malveillant : un logiciel destiné à nuire ou à abuser des ressources du système est installé (par mégarde ou par malveillance) sur le système, ouvrant la porte à des intrusions ou modifiant les données ;
- Des données confidentielles peuvent être collectées à l'insu de l'utilisateur et être réutilisées à des fins malveillantes ;
- Une mauvaise manipulation ou une malveillance entraînant une perte de matériel et/ou de données.

1.2 Rapport des contrôleurs attaqués

Nous avons un rapport pour la période du dimanche 07 aout 2022 jusqu'au mardi 06 septembre 2022, qui fournit des informations sur les attaques détectées sur les contrôleurs

logiques programmables (PLC). Ce rapport est généré pour tous les groupes.

Nous extrairons du rapport des contrôleurs attaqués le récapitulatif suivant :

- Tentative d'attaque : 00 ;
- Contrôleurs attaqués : 00 ;
- Première tentative d'exécution bloquée : N/A ;
- Dernière tentative d'exécution bloquée : N/A.

À partir des résultats obtenus, nous déduisons que le SI du CR METAL n'a pas reçu d'attaque le dernier mois. Ce que nous conduise à dire que ce SI est protégé de l'extérieur grâce à ces protocoles et équipement de sécurisation.

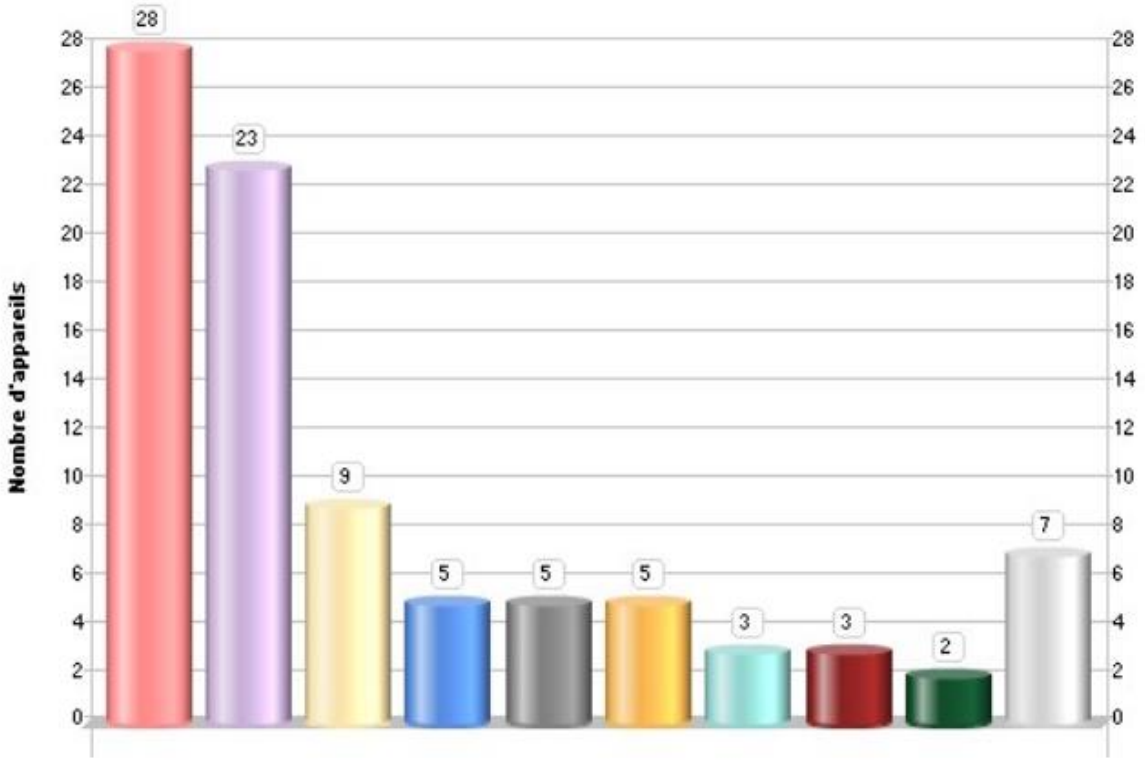
Les attaques peuvent être sous forme d'espionnage, de vole de données sensibles chiffrées, fraude, sabotage, malveillance…etc. cependant il faut prendre que CR METAL peut être attaquée de différentes manières, de la simple saturation du réseau informatique aux logiciels espions évolués.

La sécurisation du SI de CR METAL est régulièrement mise à jour, ce qu'il permettra d'améliorer sa sécurité informatique et prévenir les nouvelles formes d'attaques, aussi s'inscrire à la liste de diffusion pour les recevoir directement dans l'email.

1.3 Rapport sur l'état de la protection

Rapport du 06 septembre 2022 fournit des informations sur les états des applications de sécurité sur les appareils.

Figure 18: diagramme en bâtons sur l'état de protection.



Source : assistant SI CR METAL.

D'où le diagramme en dessus, on a :

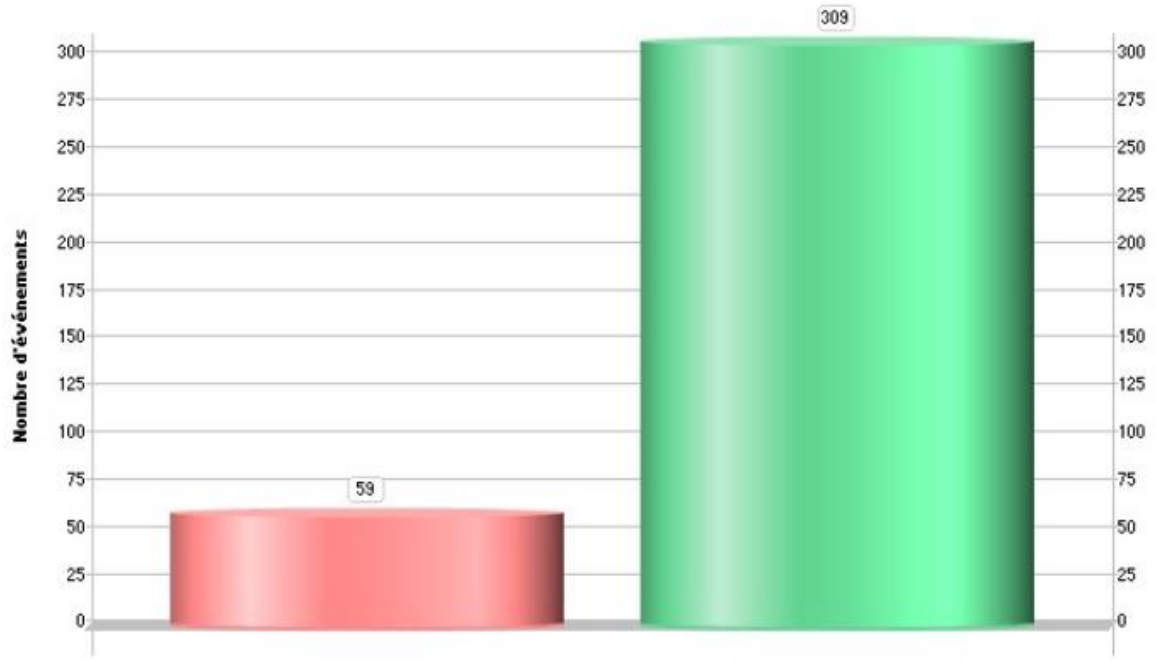
- 28 appareils : la recherche de virus n'a pas été exécutée depuis longtemps ;
- 23 appareils : la protection est désactivée ;
- 09 appareils : ne se sont pas connectés au serveur d'administration ;
- 05 menaces actives sont détectées ;
- 05 appareil : la vérification de mise à jour Windows Update n'a pas eu lieu depuis longtemps ;
- 05 appareils : la recherche de virus n'a pas été exécutée depuis longtemps ;
- 03 appareils : l'application de sécurité n'est pas en cours d'exécution ;
- 07 appareils : autres causes.

Étant donnée la multitude des facteurs causes d'agression en présence des appareils de SI du CR METAL, il est impossible de gérer parfaitement la protection parfaitement surtout en prenant en considération le comportement personnel.

1.4 Rapport sur les erreurs

Période du dimanche 07 aout 2022 jusqu'au mardi 06 septembre 2022 :

Figure 19: diagramme en battons sur les erreurs.



Source : assistant SI CR METAL.

Dont on a :

- 59 appareils avec erreurs du temps d'exécution ;
- 309 appareils ont exécuté des tâches complètes avec une erreur.

Les erreurs d'exécution sont les erreurs de Windows les plus communes, pour notre SI les causes sont présentées comme suit :

- Registre corrompu ou erreur de registre causant un dysfonctionnement de programme ;
- Drivers de l'appareil pas à jour ;
- Virus ;
- Certains fichiers ou dossiers requis pour utiliser le programme ont disparu ou ne se trouvent plus à leur place.

Afin de réparer les erreurs d'exécution, il faut procéder aux étapes suivantes :

- Identifier le fichier qui cause le problème d'exécution ;

- Supprimer le programme ou fichier en question via le gestionnaire des taches du Windows ;
- Scanner et nettoyer l'appareil, car un programme malveillant peut générer le problème d'exécution ;
- Désinstaller et réinstaller l'application ou programme problématique ;
- Restauration des données depuis un serveur endommagé.

1.5 Rapport sur les menaces

Le rapport du 06 septembre 2022 fournit des informations sur les menaces détectées sur les appareils.

Récapitulatif :

Tableau 2: tableau des types de menaces.

Objet détecté	Type d'objet	Objets infectés
Heur:trojan.win32.Générique	Cheval de trois	396
Grootcho.com	Lien malveillant	17
Hacktool.BAT.KMSAuto.m	Outil malveillant	23

Source : rapport des menaces CR METAL.

Les causes des menaces présentées dans le tableau ci-dessous, sont les principales lacunes de sécurité que nous avons constatées, à savoir :

- Une politique de gestion de mots de passe insuffisante, nous avons remarqué qu'ils ne sont pas renouvelés régulièrement ;
- Des systèmes et des applications, dont les sites web, qui ne sont pas à jour de leurs correctifs de sécurité ;
- Nous avons remarqué l'absence d'une séparation stricte des usages entre utilisateur et administrateur des réseaux ;
- Une absence de surveillance de système d'information (analyse des journaux réseaux) ;
- Un laxisme manifeste dans la gestion des droits d'accès ;
- Une ouverture excessive d'accès externes incontrôlés au système d'information (télétravail et télé administration des systèmes).

Section 2: Synthèse de résultat et recommandation

2.1 Synthèse de résultats

Au cours de notre stage au niveau de l'entreprise CR METAL, nous avons constaté pas mal d'anomalies, notamment :

2.1.1 Problématique d'information

Sans en avoir l'air, une problématique d'information correspond au problème à résoudre. Elle s'inscrit toujours dans plusieurs dimensions : organisationnelle, sociale, technique économique et cognitive :

- Problématique de mémoire, accumuler et archiver ;
- Problématique de capitalisation : expliciter, construire du sens, contextualiser (valeur ajoutée) ;
- Problématique d'exploitation (recherche, rendre accessible) ;
- Problématique d'organisation du travail et de processus ;
- Problématique de communication des flux : faire circuler, irriguer (information courante) ;
- Problématique réseau : mettre en relation, rassembler, unifier, animer.

2.1.2 Vulnérabilités du SI de CR METAL

- **Partie installation/matériel :**
  - Câbles ne sont pas identifiés et non plus protégés ;
  - Installation non hiérarchique (plusieurs switches dans même bureau) ;
  - Matériels intermédiaires du réseau sont placés dans des endroits publiques ce qui n'est pas conseiller ;
  - Aucun schéma de réseau.
- **Partie configuration/déploiement**
  - La configuration du réseau est basée sur des adresses IP statiques et non dynamiques, ce qui pose un problème de gaspillage des adresses IP par le temps ;
  - La session utilisateur est protégée par un mot de passe statique qui n'expire jamais ;
  - Installation du serveur DNS avec le serveur de base de données dans le même ordinateur et engendre le blocage total du serveur.

2.2 Recommandation

À ce titre, nous ferons une série de recommandations dont le but ultime est d'améliorer la gestion des risques de SI du CR METAL, afin de le rendre plus en plus moins vulnérable.

2.2.1 Proposition et solution pour SI du CR METAL

- **Contrôle de l'accès aux systèmes d'information :**
  - Classifier chaque information mise à disposition sur l'infrastructure informatique et l'associer à des profils d'utilisation ;
  - Interdire à l'utilisateur simple de s'identifier sur leurs postes de travail ;
  - Le responsable des ressources informatiques peut prendre sans délai les mesures nécessaires de protection.
- **Dispositions générales de sécurité :**
  - L'entreprise est dotée d'un ensemble de règles de bon usage de moyens et de principes de contrôles à protéger ses biens matériels (information) ;
  - Mettre en place une politique de sauvegarde, ce qui permet la restauration.
- **Protection des postes de travail :**
  - Les postes de travail des différents usagers doivent être munis d'un anti-virus mis à jour au moins de façon journalière ;
  - Le partage de répertoires ou de ressources du poste de travail doit être attribué aux usagers habilités sous la responsabilité de l'usager du poste ;
  - Le poste de travail doit être verrouillé lorsque son utilisateur n'est pas à son poste pour maintenir la confidentialité des informations ;
  - Le contenu des machines obsolètes qui ne sont plus utilisées doit être supprimé ;
  - L'usager doit prendre les mesures nécessaires pour protéger les données.
- **Protection des mots de passe :**
  - L'inscription de mots de passe dans des documents ;
  - Le mot de passe de l'administrateur local ou réseau doit être obligatoirement discret ;

- Identifier et cartographier les données sensibles ;
- Sécuriser l'accès et assurer la traçabilité.

- **Messagerie électronique et accès internet :**
  - L'accès à internet se fait à partir d'un serveur sécurisé ;
  - Soumettre tout mail et tout document téléchargé à une détection des virus et code malicieux.

2.2.2 Propositions pour le personnel de CR METAL

- **Former et sensibiliser le personnel :**
  - L'information du personnel est primordiale dans la réussite d'un projet de sécurisation du SI, pour qu'il en comprenne l'utilité et sache l'appliquer.
  - De manière généraliste, une bonne pratique est donc de sensibiliser l'ensemble du personnel aux enjeux de la sécurité informatique pour leur organisation.
  - Aussi il faut rappeler les engagements de l'organisation, et donner des exemples très pratiques et des procédures internes pour éviter les incidents les plus habituels.
  - Les employés directement concernés par la sécurité du SI et qui appartient au département informatique doivent être formés pour qu'ils sachent gérer et utiliser correctement les outils.

CONCLUSION

La gestion de la sécurité de l'information et la mise en place de contrôles appropriés sont devenues de plus en plus importantes, d'autant plus que l'interconnectivité entre les organisations augmente. Les organisations ont besoin d'identifier les vulnérabilités, les menaces associées et les contrôles appropriés, afin d'améliorer la performance organisationnelle.

Le travail réalisé dans le cadre de mémoire master management e-gouvernement s'inscrit dans le domaine des gestions des risques des SI, il consistait principalement à proposer un SI moins vulnérable et plus sécurisé. C'était l'objectif principal de cette étude de recherche afin de répondre à la problématique posée.

Au premier lieu, nous avons commencé par une revue de littérature sur les recherches et les études, qui ont été faites sur notre thématique, en prenant en considération deux variables principaux, qui sont management des risques et sécurité des systèmes d'information.

Ensuite, nous avons entamé le cadre théorique, dont nous avons défini les axes principaux de notre thématique de recherche, notamment : SI, gouvernance d'un SI, sécurité de l'information (outils et techniques) et gestion des risques (normes et processus).

Nous avons offert un aperçu sur les méthodes de collecte de données, qui sont l'entretien, l'observation, groupe de discussion, la recherche documentaire et l'étude de cas. Durant notre analyse et étude de recherche nous avons opté pour une méthode qualitative étude de cas, qui s'attache par définition à identifier l'ensemble des variables pertinentes à la compression du phénomène de management des risques. Afin d'avoir une vision générale de l'état de sécurité de l'organisation.

Par la suite, nous avons passé à l'évaluation de la sécurité du SI de l'organisation. Puis l'analyse et l'interprétation des résultats obtenus grâce a l'outil installé Kaspersky sécurité center. Ces résultats nous ont exhorter à constater pas mal d'anomalies et de vulnérabilités.

En perspective, dont le but ultime d'améliorer la gestion des risques de SI du CR METAL. Nous avons suggéré des recommandations de tout ce qui concerne l'accès au SI, dispositions générales de la sécurité, la protection des postes de travail et des mots de passe et la messagerie électronique et l'accès à l'internet. Ainsi nous avons eu des recommandations relativement à la formation et la sensibilisation du personnel, afin de rendre meilleur la sécurité de SI. En effet, optimiser la performance organisationnelle de l'entreprise.

Pour conclure, la performance organisationnelle dépend essentiellement de la performance de son SI, dont l'utilité d'optimiser le management des risques des SI au sein d'une entreprise. De manière générale. La majorité des responsables et directeurs ont mis l'accent sur la nécessité d'assurer la sécurité de leurs SI.

RÉFÉRENCES BIBLIOGRAPHIQUES

Bibliographie

Elidrissi, D., & Elidrissi, A. (2010). *Contribution des systèmes d'information à la performance des organisations : le cas des banques.* La Revue des Sciences de Gestion.

14001, I. (2004). Environmental management systems - Requirements with guidance for use. *International Organization for Standardization*. Geneva.

Alaoui, A. (2010). Gestion du changement, TIC et compétitivité organisationnelle : le cas de la société MBA-France. *La Revue des Sciences de Gestion*, Page 81-89.

Avanesov, E. (2009, Novembre 25). RISK MANAGEMENT IN ISO 9000 SERIES STANDARDS. *thése de doctorat*. Geneve, palais des nations.

Bohnké, S. (2010). *Moderniser son système d'information. (1er édition).* Eyrolles.

Brigitte, G. (1993). *L'information et la communication dans l'entreprise*. Bulletin des Bibliothèques de France (BFF).

Deltour, F., & Lethiais, V. (2014). L'innovation en PME et son accompagnement par les TIC : quels effets sur la performance ? *Systèmes d'information & management*, Page 45-73.

Gillet, M., & Gillet, P. (2013). *Les outils du système d'information, facteur clé de succès ou d'échec dans l'évolution des organisations : le cas des universités.* Gestion et Management Public.

GREMBO, N. (2020, Novembre 30). Risque industriel et représentation des risques. *thése de doctorat*.

ISO/IEC 27001. (2013). Information technology - Security techniques - Information security management systems - Requirements. Geneve.

Jomaa Gherib, H. (2009). Contribution de l'usage des systèmes d'information à la performance des organisations. *Thèse de doctorat*. Ecole Nationale Supérieure des

Télécommunications, Paris.

Laudon, K., & Laudon, J. (2013). Management Information Systems 13e. *IBANESS İktisat, İşletme ve Yönetim Bilimleri Kongreler Serisi–Plovdiv/Bulgaristan*, Page 06-07.

Legrenzi, C. (2015). Informatique, numérique et système d'information : définitions, périmètres, enjeux économiques. *Vie & Sciences De l'Entreprise*, Page 49-76.

Leignel, J. (2006). Gouvernance du système d'information. Nice, France.

MAHARRAR, A. (2014). La mise en place d'un système d'information formalisé . *Thèse de doctorat*. Université de Tlemcen.

MAYER, N. (2009). Model-Based Management of Information System Security Risk. *Thèse de doctorat*. Namur, Belgium.

MEZIANI, M. (2012). Contribution à la méthodologie d'intégration de la qualité dans les entreprises : Evaluation des performances managériales. *Thèse de doctorat*. Université MIRA, Béjaia.

Missaoui, I. (2009). Valeur et performance des systèmes d'information. *Cahier de Charge CIGREF(5),* Page 1-50.

Moisand, D., & De Labareyre, F. (2009). *Cobit : Pour une meilleure gouvernance des systèmes d'information.* Editions Eyrolles.

Nwamen, F. (2006). Impact des technologies de l'information et de la communication sur la performance commerciale des entreprises. *La Revue des Sciences de Gestion*, Page 11-121.

Pérez, R. (2003). La gouvernance de l'entreprise. *La découverte*.

Reix, R., Fallery, B., Kalika, M., & Rowe, F. (2016). *Systèmes d'Information et Management.* Récupéré sur In Post-Print (hal-01493256; Post-Print).: https://ideas.repec.org/p/hal/journl/hal-01493256.html

Rom, H. (1984). The philosphies of science. An introductory survey. *Oxford université*

press.

Schneier, B. (2000). *degital security in a network world*. Carol Long.

Stoneburner, G., Goguen, A., & Feringa, a. (2002). *Risk Management Guide for*. NIST Special Publication.

Stoneburner, G., Hayden, C., & Feringa, A. (2004). engineering principles for information technology security (a baseline for achieving security). Gaithersburg.