MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

ÉCOLE NATIONALE SUPÉRIEURE DE Management

ENSM. Pôle Universitaire de KOLÉA

PROJET DE FIN D'ETUDES

Master en Management stratégique et système d'information

Gestion des Risques lors d'une activité d'Audit

Etude de cas « KPMG »

Élaboré par :

Ikram ABDELLI

Kenza AIT MESSAOUDENE

Encadré par :

Pr Messaoud ZEROUTI

Année universitaire 2023/2024

RÉSUMÉ

L'évolution rapide des technologies de l'information (IT) et leur intégration croissante dans les processus d'affaires des entreprises rendent impérative une gestion efficace des risques informatiques. Cette nécessité est accentuée par la cybersécurité et les nouvelles technologies, qui posent des défis supplémentaires en matière de gouvernance des systèmes d'information. Cette recherche vise à explorer la gestion des risques dans le contexte de l'audit IT et de la gouvernance des technologies de l'information (IT), en examinant les méthodes et approches existantes pour identifier, évaluer et traiter les risques informatiques.

Une revue de littérature approfondie a été menée pour analyser divers articles et études sur la gestion des risques IT, l'audit et des méthodes utilisées pour sa réalisation. Cette recherche s'appuie sur la méthode MEHARI et sur des entretiens semi-directifs avec les auditeurs de KPMG et l'équipe de la Direction des Systèmes d'Information (DSI).

Mots clés : Gestion des risques, audit IT, gouvernance des technologies de l'information, MEHARI.

ABSTRACT

The rapid evolution of information technology (IT) and its increasing integration into business processes make effective management of IT risks imperative. This necessity is heightened by cybersecurity and new technologies, which pose additional challenges for the governance of information systems. This research aims to explore risk management in the context of IT audit and IT governance by examining existing methods and approaches for identifying, assessing, and addressing IT risks.

A comprehensive literature review was conducted to analyze various articles and studies on IT risk management, auditing, and the methods used for these purposes. This research is based on the MEHARI method and semi-structured interviews with auditors from KPMG and the Information Systems Department (DSI) team.

Keywords: Risk management, IT audit, IT governance, MEHARI.

ملخص

إن التطور السريع لتكنولوجيا المعلومات وإدماجها المتزايد في العمليات التجارية للشركات يجعل الإدارة الفعالة لمخاطر تكنولوجيا المعلومات أمراً حتمياً. وتشتد هذه الحاجة بسبب الأمن السيبراني والتكنولوجيات الجديدة التي تطرح تحديات إضافية فيما يتعلق بحوكمة نظم المعلومات. يهدف هذا البحث إلى استكشاف إدارة المخاطر في سياق تدقيق تكنولوجيا المعلومات وحوكمة تكنولوجيا المعلومات، من خلال دراسة الأساليب والنهج الحالية لتحديد مخاطر تكنولوجيا المعلومات وتقييمها ومعالجتها.

تم إجراء مراجعة شاملة للأدبيات لتحليل مختلف المقالات والدراسات حول إدارة مخاطر تكنولوجيا المعلومات والتدقيق والأساليب المستخدمة لهذه الأغراض. ويستند هذا البحث إلى طريقة MEHARI والمقابلات شبه المنظمة مع مدققي الحسابات من شركة KPMG وفريق إدارة نظم المعلومات (DSI).

الكلمات المفتاحية: إدارة المخاطر، تدقيق تكنولوجيا المعلومات، حوكمة تكنولوجيا المعلومات، MEHARI

REMERCIEMENT

Avant tout, nous exprimons notre profonde gratitude au bon Dieu pour le courage et la patience qui nous ont permis de mener à bien ce travail.

Nous adressons nos sincères remerciements à notre encadrant, Monsieur Messaoud ZEROUTI, dont le soutien constant, la patience et les conseils avisés ont été essentiels à l'achèvement de ce projet.

Nos remerciements vont également à Monsieur Derrar, dont l'enseignement inspirant et les précieux éclairages ont considérablement enrichi notre démarche de recherche. Son expertise a été cruciale pour la réalisation de ce travail.

Nous tenons à exprimer notre reconnaissance à toutes les personnes qui ont contribué de près ou de loin à la réalisation de ce projet, avec une mention spéciale pour Monsieur Kezzim et Madame Toumi.

Nous remercions également les membres du jury pour avoir accepté de lire et d'évaluer ce mémoire. Enfin, nous adressons nos remerciements à l'ensemble des enseignants de l'École Nationale Supérieure de Management, qui ont rendu notre formation enrichissante tant sur le plan personnel qu'académique.

Kenza

À mes chers parents,votre soutien constant et vos sacrifices ont été les fondations sur lesquelles j'ai pu bâtir mon chemin vers la réussite. Votre présence aimante a été ma source d'inspiration et ma force motrice dans les moments de doute. Pour tous cela et bien plus encore je vous suis infiniment reconnaissante.

À mon frère et mes sœurs(Mohammed,Cyrine,Ikram,Méliza), votre présence et vos encouragements ont été une source constante de soutien, me donnant la force de persévérer. À ma nièce et mon neveu(Massilia,Mahdi Aksil) votre innocence et votre joie m'inspirerons toujours.

À tous mes amis, ceux qui ont été là avant et ceux qui m'ont rejoint en cours de route, je vous suis reconnaissante pour votre amitié et votre soutien indéfectible. Vos encouragements, vos

rires et vos conseils m’ont permis d’être qui je suis aujourd’hui. Vous êtes une partie précieuse de ma vie, et je vous remercie du fond du cœur pour tout ce que vous m’avez apporter.

Ikram

Je tiens à adresser un remerciement particulier à mes parents. Leur soutien, leur amour inconditionnel et leurs encouragements constants ont été ma source de force et d'inspiration et m'ont permis d'atteindre ce moment. Toujours à mes côtés, ils m'ont soutenu et encouragé à persévérer sans jamais faiblir. Que Dieu les protège.

Je suis également reconnaissant envers ma chère tante Hassina qui est comme une seconde mère pour moi, mes cousines Aya, Amira, Manel, Ayla et mon cousin Larbi, qui sont bien plus que des cousins pour moi. Ils ont toujours été là pour moi, pour partager mes joies et mes peines, et pour me faire rire même dans les moments les plus sombres. Leur présence est précieuse pour moi, et je suis chanceux de les avoir dans ma vie.

À tous mes ami(e)s, j'exprime ma sincère gratitude pour avoir enrichi ma vie par leur présence, leur soutien constant, et leur bienveillance. Leur amitié et les moments partagés ont été une source inestimable de force et de bonheur pour moi. Je vous remercie de tout cœur pour avoir été là dans les moments de joie comme dans les moments difficiles.

TABLE DES MATIERES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES ABRÉVIATIONS, SIGLES ET ACRONYMES

AFNOR : Association Française de Normalisation

ADELI : Association pour le Développement de l'Économie par l'Informatique

CMMI: Capability Maturity Model Integration

COBIT: Control Objectives for Information and related Technology

COSO : Committee of Sponsoring Organizations

DCSSI : Direction Centrale de la Sécurité des Systèmes d'Information

D, I, C : Disponibilité, Intégrité, Confidentialité

DSI : Directeur des Systèmes d'Information

EBIOS : Expression des Besoins et Identification des Objectifs de Sécurité

ERM : Enterprise Risk Management (Gestion des Risques d'Entreprise)

ERP : Enterprise Resource Planning

ESI : École Supérieure d'Informatique

FERMA: Federation of European Risk Management Associations

IA : Intelligence Artificielle

IIA : Institute of Internal Auditors

ISA : International Standards on Auditing

ISACA: Information Systems Audit and Control Association

ISO : International Organization for Standardization

IT: Information Technology (Technologies de l'Information)

ITGI: Information Technology Governance Institute

ITIL: Information Technology Infrastructure Library

KPMG: Klynveld Peat Marwick Goerdeler (nom de la firme de services professionnels)

MEHARI : Méthode Harmonisée d'Analyse des Risques Informatiques

OCTAVE: Operationally Critical Threat, Asset, and Vulnerability Evaluation

PDG : Président Directeur Général

RAM : Random Access Memory

RSSI : risques de sécurité de système d'information

SEI : Software Engineering Institute

SI : Systèmes d'Information

SP : Système de Pilotage

SO : Système Opérant

VPN : Virtual Private Network

ClUSIF : Club des Utilisateurs de la Sécurité des Systèmes d'Information

EGIT : Excellence en Gouvernance des Technologies de l'Information

IoT : Internet des Objets

INTRODUCTION

Dans cette introduction, nous commencerons par présenter le contexte de la recherche, ses objectifs ainsi que sa contribution sur le plan théorique et managérial. Ensuite, nous exposerons notre plan de travail.

Dans le contexte actuel, les technologies de l'information (IT) jouent un rôle central dans les IT opérations commerciales. La gestion efficace des risques liés aux IT est cruciale pour les organisations, car les failles de sécurité informatique peuvent entraîner d'importantes pertes financières, des dommages à la réputation et des interruptions d'activité.

L'audit IT se positionne comme une composante essentielle de la gouvernance IT au sein des entreprises. Son objectif est d'aligner les objectifs informatiques sur les objectifs stratégiques de l'entreprise, de gérer les risques et de garantir la conformité.

Concrètement, l'audit IT agit comme un outil de la gouvernance IT en fournissant une évaluation indépendante et approfondie des processus, systèmes et contrôles informatiques de l'entreprise. Elle vérifie si les politiques et procédures définies dans le cadre de la gouvernance IT sont effectivement mises en œuvre et respectées, identifiant ainsi les lacunes ou les risques potentiels nécessitant une attention particulière.

Dans ce contexte, notre objectif de recherche est d'approfondir notre compréhension de la gouvernance des technologies de l'information ainsi que du rôle de l'audit IT, en mettant particulièrement l'accent sur quelques méthodes qui peuvent être déployé en mission d'audit. Nous nous pencherons également sur les pratiques actuelles de KPMG dans ce domaine. En éclairant les aspects essentiels, notre ambition est de contribuer activement à l'amélioration continue des processus de gouvernance des IT et à renforcer la position de KPMG en tant que leader dans le domaine de l'audit et du conseil.

Cette recherche présente une pertinence théorique en contribuant à l'avancement des connaissances dans le domaine de la gouvernance des IT et de la gestion des risques, tout en offrant des recommandations pratiques et exploitables pour les entreprises clientes de KPMG, ce qui en fait une étude précieuse tant sur le plan théorique que managérial.

La recherche proposée s'inscrit dans le domaine de la gouvernance des risques liés aux technologies de l'information (IT), et elle vise à enrichir la base théorique de plusieurs manières :

- En élargissant la compréhension des processus de gestion des risques et des méthodes utilisées pour assurer son optimisation.
- En explorant le rôle de l'audit IT dans l'évaluation et l'amélioration de la gouvernance des risques IT.

La question de recherche a une pertinence directe pour les praticiens de la gestion des risques et de la gouvernance des IT, en particulier pour les entreprises qui s'appuient sur des services d'audit IT fournis par des sociétés telles que KPMG. En fournissant des recommandations spécifiques basées sur les résultats de l'audit IT et les meilleures pratiques, la recherche offre :

- un cadre pour l'amélioration des processus de gouvernance des risques liés aux IT au sein des organisations clientes de KPMG.
- permet également à ces organisations de mieux comprendre les contrôles d'audit IT réalisés par KPMG et de tirer parti de ces connaissances pour renforcer leur posture en matière de gouvernance des IT et de gestion des risques.

1. Question de la recherche

La question à examiner et pour laquelle nous chercherons à fournir une réponse est la suivante: **Comment assurer une bonne gestion des risques en matière d'IT et quelles recommandations peuvent être formulées à la suite d'une activité d'audit IT pour un client de KPMG ?**

Sous-questions :

- Quels sont les contrôles de l'audit IT réalisé par KPMG concernant la gestion des risques liés aux IT chez le client ?
- Comment la méthode MEHARI peut-elle être adaptée pour répondre aux besoins spécifiques de l'audit IT ?
- Quels sont les avantages et les limites de l'application de la méthode MEHARI dans le processus de gestion des risques lors de l'audit IT pour les clients de KPMG?
- Quelles recommandations spécifiques peuvent être proposées pour améliorer la gouvernance des risques liés aux IT chez le client en tenant compte des résultats de l'audit IT?

2. Plan de travail

Notre recherche est articulée de la manière suivante :

Nous commençons notre étude par une introduction éclairant l'intérêt et les objectifs de notre thème, en plus de présenter la problématique et la méthodologie adoptée dans cette investigation.

Ensuite, trois chapitres sont déployés de la manière suivante :

Le premier chapitre se consacre à la revue de la littérature et au cadre conceptuel, où nous apportons des définitions précises des concepts clés liés à notre sujet.

Le deuxième chapitre s'attache à décrire la méthodologie de recherche employée et le contexte organisationnel dans lequel nous avons mené notre étude.
Le troisième chapitre expose les résultats issus du terrain, suivis d'une discussion approfondie de ces derniers.

Enfin, nous concluons notre recherche en synthétisant les principaux résultats obtenus, et en identifiant les limitations inhérentes à cette étude.

CHAPITRE I : REVUE DE LITTÉRATURE ET CADRE CONCEPTUEL

Ce chapitre débutera par une revue de littérature, suivie par la présentation du cadre conceptuel de notre recherche, mettant en avant les principaux concepts utilisés.

1. Revue de littérature

1.1 La gestion des risques

La gestion des risques est un domaine crucial pour toute organisation, qu'elle soit publique ou privée. Elle vise à anticiper, évaluer et maîtriser les risques susceptibles d'affecter ses activités, sa réputation et sa pérennité.

La littérature actuelle souligne l'importance cruciale de la gestion des risques. Deux articles récents mettent en évidence différents aspects de ce domaine ainsi que deux autres articles examinant les différentes solutions ou méthodes permettant de sécuriser un système d'information.

Le premier article intitulé « Comment construire des échelles de cotation des risques » de Amanda Wanderley, Publié en 2023 se concentre sur l'utilisation des échelles dans la gestion efficace des risques. Il met en avant le rôle essentiel de ces échelles pour fournir une évaluation objective de la gravité potentielle des risques, qu'ils soient positifs ou négatifs. En évaluant la gravité des risques, les entreprises peuvent hiérarchiser leur gestion en fonction de leur criticité, ce qui permet une prise de décision plus éclairée et proactive. L'article souligne également l'importance de définir des critères spécifiques à l'organisation pour garantir une compréhension commune lors de l'évaluation des risques.

Le deuxième article intitulé « Qu'est-ce que la gestion des risques ? » publié la même année par la même auteure aborde la gestion des risques dans son ensemble, en mettant en lumière son rôle dans la maîtrise des effets des risques sur l'organisation. Il décrit la gestion des risques comme un processus proactif visant à identifier, évaluer et piloter les risques susceptibles de perturber une organisation. En décomposant le processus de gestion des risques en plusieurs étapes, telles que l'identification, l'analyse, l'évaluation, le traitement et le contrôle continu des risques, l'article démontre comment les entreprises peuvent gérer efficacement les risques auxquels elles sont confrontées.

Les deux articles soulignent également l'importance de distinguer entre la gestion des risques et le management des risques, ainsi que les avantages de la gestion des risques, tels que la prise de décisions éclairées, la protection contre les menaces et l'exploitation des opportunités.

Concernant les méthodes utilisées deux articles examinent des aspects différents mais complémentaires de la gestion des risques liés à la sécurité des systèmes d'information et à l'amélioration de la performance des PME.

L'article de Khaled Benantar, Souad Benmeziane et Omar Deghbar se concentre sur une étude comparative des méthodes de gestion des risques, en mettant en lumière les méthodologies MEHARI, Ebios et Octave, ainsi que les normes internationales telles que l'ISO 27005:2008.
Selon l'auteur, MEHARI peut être un outil précieux pour la gestion de projets informatiques, mais comme toute méthode, elle nécessite une compréhension approfondie et une adaptation intelligente aux besoins et aux contraintes de chaque projet.
Dans l'ensemble, la méthode Méhari a ses avantages et ses inconvénients. Parmi ses points forts, on peut citer sa focalisation sur les besoins réels des utilisateurs, sa flexibilité grâce à son approche itérative, et son orientation vers la gestion des risques, ce qui permet de mieux anticiper les éventuels problèmes.
Cependant, il a mentionné quelques critiques soulignent que la méthode Méhari peut être complexe à mettre en œuvre, surtout pour les équipes peu expérimentées. De plus, son efficacité peut varier en fonction du contexte et de la nature spécifique du projet.
D'autre part, l'article de Driss Helmi et Kamel Kaya explore comment améliorer la performance des PME en réduisant les risques, notamment en intégrant l'intelligence artificielle (IA). Les auteurs soulignent l'importance de l'anticipation des difficultés pour mieux gérer les incertitudes environnementales et s'adapter aux évolutions du système d'information. Ils décrivent MEHARI comme une méthode couramment utilisée comprenant trois processus (identification des risques, évaluation et gestion des risque), avec une emphase sur l'ajout de la communication comme processus transversal. L'article insiste sur l'importance d'une politique de sécurité bien définie, centrée sur la gestion des risques, pour protéger les systèmes d'information et contribuer à la création de valeur, tout en soulignant le rôle crucial de la gestion des risques dans la fonction maintenance pour l'amélioration continue de la performance et la réduction des coûts.

En résumé, les deux articles mettent en évidence l'importance de la gestion des risques pour la sécurité des systèmes d'information et la performance des entreprises, en soulignant différentes méthodologies et approches pour y parvenir. Les résultats des deux études mettent en évidence les points forts et les limites de chaque méthode de gestion des risques, ainsi que les différences significatives entre elles. Cette analyse comparative fournit des informations précieuses pour

les praticiens de la sécurité informatique qui cherchent à choisir la méthode la plus adaptée à leurs besoins spécifiques.
Cependant, bien qu'ils fournissent des informations utiles, ils sont limités par le nombre restreint de méthodologies étudiées et le manque de directives spécifiques sur leur application.

L'étude menée par KPMG, intitulée "Gestion des risques, Audit et Contrôle Internes - Risques émergents et nouvelles technologies", réalisée en novembre 2018, offre une perspective précieuse sur les défis actuels de la gouvernance des systèmes d'information (SI), de l'audit IT et de la gestion des risques. L'enquête interroge les membres clés de la gouvernance d'entreprise, de l'audit interne et des finances sur leurs perceptions des risques majeurs, les attentes à l'égard de l'audit interne, l'impact des nouvelles technologies sur l'audit interne, ainsi que les compétences essentielles à renforcer au sein des équipes. Les résultats mettent en lumière l'importance croissante de l'audit des technologies de l'information, soulignant la nécessité d'intégrer les risques émergents liés aux IT dans les plans d'audit et de surveiller l'efficacité des dispositifs de gestion des risques dans ce domaine. Cette étude confirme ainsi l'importance stratégique de la cybersécurité, des nouvelles technologies et de la digitalisation dans le contexte actuel des entreprises. Afin de mieux comprendre ce domaine, une revue de littérature approfondie est nécessaire pour explorer ces différents principes

1.2 La gouvernance IT et gestion des risques

Nous avons examiné de près un événement qui s'est déroulé le 8 juin 2022 de 11h à 12h15 : un webinaire entre l'École Supérieure d'Informatique (ESI) et Optimum Télécom Algérie, pour le personnel de l'entreprise. Dirigé par le Professeur Ghomari A.R, ce webinaire a exploré un sujet essentiel : la manière dont les entreprises gèrent leurs systèmes informatiques, considérés comme un aspect clé du bon fonctionnement des entreprises.

Dans un premier temps, l'orateur a replacé le contexte en rappelant les préoccupations antérieures des entreprises concernant la gestion de leur système informatique. Par la suite, il a examiné en détail les principaux domaines la gouvernance I&T, notamment l'importance de l'alignement des objectifs de l'entreprise avec la technologie, la capacité des systèmes informatiques à ajouter de la valeur, la gestion des risques, l'optimisation des ressources et l'évaluation continue des performances. De plus, il a offert des perspectives sur la manière de mettre en œuvre ces bonnes pratiques dans le cadre des projets informatiques.

Enfin, le webinaire a abordé les défis contemporains auxquels les entreprises sont confrontées en matière de gestion des risques technologiques, en mettant en lumière les dernières recherches dans ce domaine. Parmi les sujets discutés figuraient la gestion des services informatiques basés sur le Cloud, ainsi que l'implication et la collaboration des employés dans les projets informatiques, en soulignant leur importance dans la réduction des risques et l'amélioration de la résilience de l'entreprise face aux menaces technologiques émergentes.

La littérature sur la gouvernance des technologies de l'information (IT) et la gestion des risques souligne l'importance croissante pour les organisations de comprendre et de gérer les risques liés à leur dépendance à l'égard des IT. Bowen et al. (2007) mettent en évidence les préoccupations croissantes des directions supérieures concernant les risques significatifs associés à l'utilisation d'Internet, susceptibles de perturber les objectifs organisationnels. Les incidents et les défaillances des systèmes informatiques, comme le soulignent Hughes (2006) et Trautmann, Triche et Wetherbe (2013), peuvent déclencher des crises graves, entraînant des dommages à la réputation, des pertes financières et des responsabilités légales.

Dans ce contexte, la littérature insiste sur la nécessité pour les organisations de gérer efficacement les risques informatiques, en se concentrant sur la protection des actifs informatiques, la reprise après sinistre et la continuité opérationnelle (Maizlish & Handler, 2005). La création de valeur informatique étant primordiale pour les entreprises, la gestion des risques informatiques vise à préserver cette valeur (Van Grimbergen et al., 2004). La gouvernance des IT est identifiée comme un moyen crucial de gérer ces risques (Weill & Ross, 2004), soulignant l'importance pour la direction supérieure de comprendre et de reconnaître ces risques pour assurer leur maîtrise.

Pour une gouvernance des IT efficace, il est nécessaire de valider et de gérer correctement les risques, en mettant en place des contrôles pour identifier et éliminer les causes potentielles des problèmes, ainsi que pour surveiller les événements déclencheurs afin d'atténuer leurs effets et cela à travers l’audit interne (Calder dans Bradley et al., 2012a). En intégrant des mécanismes tels que COBIT et la gestion des risques d'entreprise (ERM), les risques peuvent être gérés de manière proactive (Wallace, Keil et Rai, 2004 ; Huang et al., 2011). Ainsi, la littérature souligne l'importance cruciale d'une approche stratégique et bien structurée de la gouvernance des IT

pour permettre aux entreprises de gérer efficacement les risques liés à leur dépendance croissante aux technologies de l'information.

En conclusion, la gouvernance des systèmes informatiques est un élément essentiel pour les entreprises d'aujourd'hui qui cherchent à exploiter au maximum le potentiel des technologies de l'information tout en minimisant les risques associés. En s'inspirant des bonnes pratiques et des leçons tirées des études de cas, les entreprises peuvent mettre en place une gouvernance des OT++IT efficace qui contribue à la création de valeur, à la protection des actifs et à la réalisation des objectifs stratégiques.

1.3 Audit et gestion des risques

Plusieurs articles ont été consacrés à la gestion des risques, chacun proposant des approches distinctes pour aborder cette problématique complexe.

L'article intitulé "Contribution de l'audit dans la gestion des risques liés aux systèmes d'information dans le cadre de la gouvernance des systèmes d'information - Cas Evolutec International – Algérie", rédigé par Abdelouahed Mohamed, étudiant doctorant en Comptabilité à l'Université Mohamed Khider de Biskra, et Dr Ahmed Gaid Noureddine de la même université, offre une analyse détaillée du processus opérationnel spécifique mis en place chez Evolutec International en 2017 pour gérer les risques des systèmes d'information (SI). Ce processus débute par l'identification minutieuse des risques potentiels, consignés dans un registre dédié, suivi d'une évaluation rigoureuse prenant en compte la probabilité et l'impact de ces risques. Par la suite, une série de stratégies de réponse est proposée, incluant l'évitement, la réduction, le partage ou encore l'acceptation des risques, tout en prenant en considération les niveaux de tolérance au risque et les responsabilités associées. Le plan d'action élaboré à la suite de cette évaluation est ensuite mis en œuvre avec une surveillance continue pour garantir son efficacité. De plus, l'article présente les résultats d'un audit interne spécifiquement axé sur les risques SI de l'entreprise, mettant en lumière les lacunes identifiées et fournissant des recommandations ciblées pour améliorer la gestion de ces risques.

En revanche, le deuxième article, intitulé "CADRE DE RÉFÉRENCE DE LA GESTION DES RISQUES", élaboré par FERMA en 2011, adopte une approche plus générale du processus de gestion des risques, mettant l'accent sur les principes et les étapes clés applicables à une variété

d'organisations. Il met en évidence des éléments essentiels tels que l'évaluation du risque, le traitement du risque, la communication et le reporting sur les risques, ainsi que la nécessité d'une politique écrite de gestion des risques, de l'engagement de la direction, de la formation et du développement de la sensibilité aux risques chez toutes les parties prenantes. De plus, il propose des exemples de techniques d'identification et d'analyse des risques, offrant ainsi un panorama exhaustif du domaine de la gestion des risques sans se concentrer sur un cas spécifique.

Enfin, le troisième article, intitulé "Prise de position de l'IIA : Les trois lignes de maîtrise pour une gestion des risques et un contrôle efficaces", datant de janvier 2013, aborde la nécessité d'une coordination rigoureuse entre les différentes fonctions impliquées dans la gestion des risques et le contrôle au sein d'une organisation, dans le cadre du processus de gouvernance. L'article souligne l'importance cruciale de trois lignes de maîtrise distinctes : les managers, les fonctions de gestion des risques et de conformité, et l'audit interne, chacune jouant des rôles spécifiques dans le processus de gouvernance. Il met également en avant l'impératif d'une surveillance efficace du système de gestion des risques par les organes de gouvernance, ainsi que la nécessité d'une coordination étroite entre les différentes lignes de maîtrise pour garantir une gestion des risques optimale.

Comparativement aux deux premiers articles, cet article de l'IIA offre une perspective plus holistique et axée sur la coordination des différentes fonctions impliquées dans la gestion des risques, mettant en lumière l'importance d'une approche intégrée pour une gestion des risques et un contrôle efficace au sein des organisations.

L'analyse d'articles et d'études révèle l'importance croissante de la gouvernance des systèmes d'information (SI), de la gestion des risques et de l'audit interne dans les organisations modernes, à l'ère du numérique. En effet, les entreprises dépendent de plus en plus des technologies de l'information pour leurs opérations critiques, ce qui rend ces domaines essentiels pour leur réussite.

Ces recherches soulignent le rôle stratégique de la cybersécurité, des nouvelles technologies et de la digitalisation pour les entreprises d'aujourd'hui. La gouvernance des IT joue un rôle crucial

en permettant d'aligner les objectifs organisationnels sur les technologies, de gérer les risques et d'optimiser les performances.

Cependant, plusieurs défis subsistent. Il est nécessaire d'adopter une approche holistique pour comprendre la relation entre la gouvernance des SI et la performance organisationnelle. De plus, des méthodologies de gestion des risques plus robustes et de meilleures pratiques d'audit interne sont nécessaires pour faire face aux menaces émergentes.

En conclusion, la gouvernance des IT et la gestion des risques doivent être au cœur des stratégies commerciales pour assurer la viabilité, la sécurité et la réussite à long terme des organisations dans un environnement numérique en constante évolution.

2. Cadre conceptuel

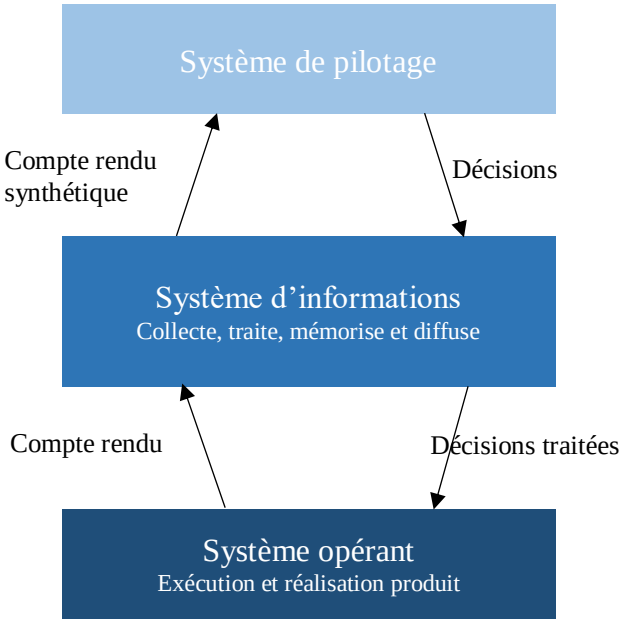
2.1 Système d'information

2.1.1 Définition

Selon (Kroenke, mesaglio, 2010) le système d'information est définie comme suit :
"Un ensemble organisé de ressources (composants matériels, logiciels, données, ressources humaines et procédures) qui permet de collecter, stocker, traiter, distribuer et utiliser l'information afin de soutenir les opérations, la prise de décision et la gestion d'une organisation."

L'organisation peut se décomposer en 3 sous-systèmes : le système de décision, le système d'information et le système opérant. Chaque système apporte des services à l'autre.

Figure 1: Le modèle opérant, information et décision



Source : (Guibert, 2007)

Système de pilotage:

- Situé au sommet du schéma, le système de pilotage (SP) représente la direction stratégique de l'organisation. Il définit les objectifs globaux et les orientations à suivre pour l'ensemble du système.
- Le SP est composé de l'équipe dirigeante et des responsables clés qui élaborent les plans stratégiques, prennent les décisions majeures et allouent les ressources nécessaires à l'atteinte des objectifs.

Système d'information:

- Le système d'information (SI) joue un rôle central dans la collecte, le traitement, le stockage et la distribution de l'information au sein de l'organisation.
- Il est composé des ressources matérielles et logicielles nécessaires à la gestion de l'information, telles que les ordinateurs, les serveurs, les réseaux, les bases de données et les logiciels d'application.
- Le SI assure la liaison entre le système de pilotage et le système opérant en fournissant aux dirigeants les informations nécessaires à la prise de décision et au pilotage de l'organisation.

Système opérant:

- Le système opérant (SO) regroupe les activités quotidiennes et les processus opérationnels de l'organisation.
- Il est composé des différents départements et services opérationnels, tels que la production, la vente, le marketing, la finance et les ressources humaines.
- Le SO utilise les informations provenant du SI pour effectuer ses tâches quotidiennes, telles que la gestion des commandes, la production de biens et services, la communication avec les clients et la gestion des finances.

2.1.2 Sécurité des systèmes d'information

La sécurité des systèmes d'information, telle que définie par le Clusif (Club des Utilisateurs de la Sécurité des Systèmes d'Information), englobe un ensemble de mesures préventives et réactives visant à protéger les systèmes d'information contre une diversité de menaces, tant internes qu'externes. Cette définition met en lumière plusieurs points essentiels :

- Protection contre les menaces : La sécurité des SI vise à prévenir les attaques telles que les malwares, les intrusions, les fuites de données et les dénis de service, assurant ainsi la continuité des opérations et la préservation de l'intégrité des données.
- Mesures préventives et réactives : Elle inclut à la fois des actions préventives, comme l'implémentation de contrôles d'accès et de sauvegardes de données, et des mesures réactives, telles que la gestion des incidents et la reprise après sinistre, pour atténuer les impacts d'éventuelles violations de sécurité.
- Systèmes d'information : La sécurité des SI s'applique à tous les composants du paysage informatique, incluant les ordinateurs personnels, les serveurs, les réseaux et les applications, afin de garantir une protection globale.

Le modèle de référence proposé par le Clusif pour la sécurité des SI comprend les domaines suivants :

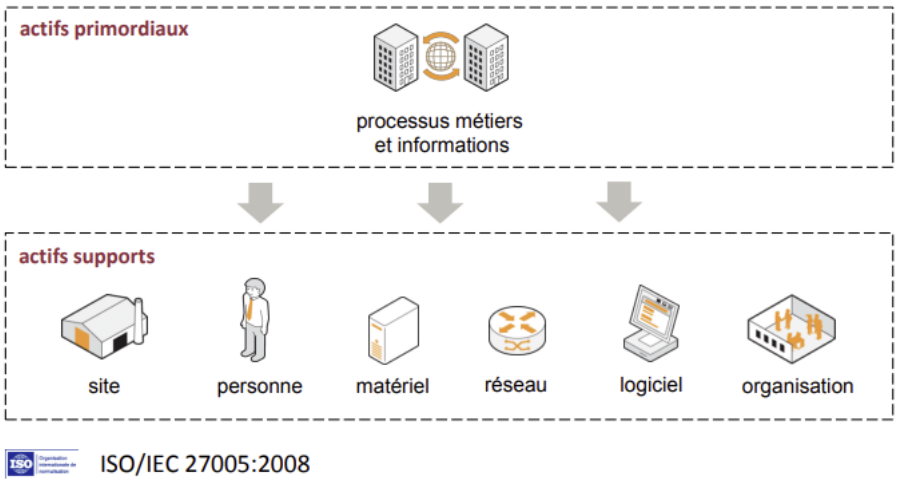
- Gouvernance : Une gouvernance efficace assure l'intégration de la sécurité dans l'ensemble des processus organisationnels, garantissant une prise de décision éclairée et une allocation adéquate des ressources
- Gestion des risques : Identifier, évaluer et traiter les risques associés à la sécurité des SI permet de prioriser les actions et d'optimiser l'efficacité des mesures de sécurité.
- Architecture et ingénierie : Concevoir des systèmes d'information sécurisés dès leur conception assure une protection proactive contre les menaces potentielles.
- Identité et gestion des accès : Contrôler l'accès aux ressources informatiques en gérant efficacement les identités et les autorisations contribue à prévenir les compromissions de sécurité.
- Protection des données : Assurer la confidentialité, l'intégrité et la disponibilité des données sensibles est essentiel pour prévenir les violations de sécurité et maintenir la confiance des parties prenantes.
- Surveillance et réponse aux incidents : La détection précoce des incidents de sécurité, associée à une réponse rapide et efficace, permet de limiter les dommages potentiels et de rétablir rapidement la normalité des opérations.

2.1.3 Les enjeux de la sécurité des SI

Le Système d'Information (SI) englobe toutes les ressources nécessaires à la collecte, à la classification, au stockage, à la gestion et à la diffusion des informations au sein d'une organisation. L'information est fondamentale, étant le moteur principal pour toutes les entreprises, administrations et organisations. Le SI doit donc être conçu pour soutenir et faciliter la mission de l'organisation.

Selon ISO/IEC 27005 :2008, le système d'information d'une organisation contient un ensemble d'actifs :

Figure 2: Niveaux de sécurité des actifs d'une organisation



✓ La sécurité du S.I. consiste donc à assurer la sécurité de l'ensemble de ces actifs.

L'objectif de la sécurité est de minimiser les risques qui pèsent sur le système d'information afin de limiter leur impact sur le fonctionnement et les activités commerciales des organisations. La gestion de la sécurité au sein du système d'information vise à :

✓ Améliorer la qualité de service attendue par les utilisateurs.
✓ Assurer au personnel le niveau de protection auquel ils ont droit.

2.1.4 La sécurité informatique

L'objectif de la sécurité informatique est de maintenir à un niveau approprié les garanties suivantes :

- **Disponibilité :** Assurer que les entités autorisées ont un accès continu aux éléments concernés.

- **Intégrité :** Veiller à ce que les ressources soient exactes et complètes, sans altération.
- **Confidentialité :** Assurer que les ressources sont accessibles uniquement aux entités autorisées, selon les besoins.
- **Traçabilité :** Garantir que les accès et les tentatives d'accès aux ressources sont enregistrés et que ces enregistrements sont conservés et exploitables.
- **Preuve :** La preuve est la qualité d'un bien nécessitant une protection adéquate, permettant de retracer, avec une confiance suffisante, les circonstances dans lesquelles ce bien évolue.

Ces cinq principes combinés, connus sous l'acronyme "DICTP", assurent un niveau de sécurité adéquat pour répondre aux besoins de sécurité des données de l'entreprise concernée.

Pour minimiser les risques technologiques et garantir la sécurité des systèmes d'information, diverses mesures doivent être mises en place dans les domaines suivants :

- **Sécurité physique :** Concernant les aspects matériels et environnementaux tels que les locaux, l'alimentation électrique et la climatisation. Cela nécessite la mise en œuvre de normes de sécurité, de protections diverses, de traçabilité des entrées, de gestion des accès, de redondance physique et de marquage des matériels.
- **Sécurité logique :** Englobant les mécanismes logiciels de sécurité, le contrôle d'accès logique comprenant l'identification, l'authentification et l'autorisation, ainsi que la protection des données par le cryptage, les antivirus et les sauvegardes.
- **Sécurité applicative :** Visant à prévenir les erreurs de programmation en mettant en place des méthodologies de développement telles que des plans de contrôles et de tests, ainsi que des plans de migration des applications.
- **Sécurité de l'exploitation :** Axée sur le bon fonctionnement des systèmes à travers des procédures de maintenance, de test, de diagnostic, de mise à jour, ainsi que des plans de sauvegarde et de secours.
- **Sécurité des télécommunications :** Impliquant la sécurisation de l'infrastructure réseau au niveau des accès, des protocoles, des systèmes d'exploitation et des équipements.

2.2 Gouvernance

2.2.1 La gouvernance IT, son importance et ses objectifs

2.2.1.1 Gouvernance

- La gouvernance renvoie à un système d'entités décisionnelles qui dirige un certain domaine d'activités. Cela implique notamment une structure de gouvernance et un dynamisme de système (processus de gouvernance, activités de gestion, etc.) (dictionnaire Larousse).
- 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-droits (actionnaires) et les acteurs. (COBIT 2019 Framework" (publié par ISACA))

2.2.1.2 La gouvernance IT

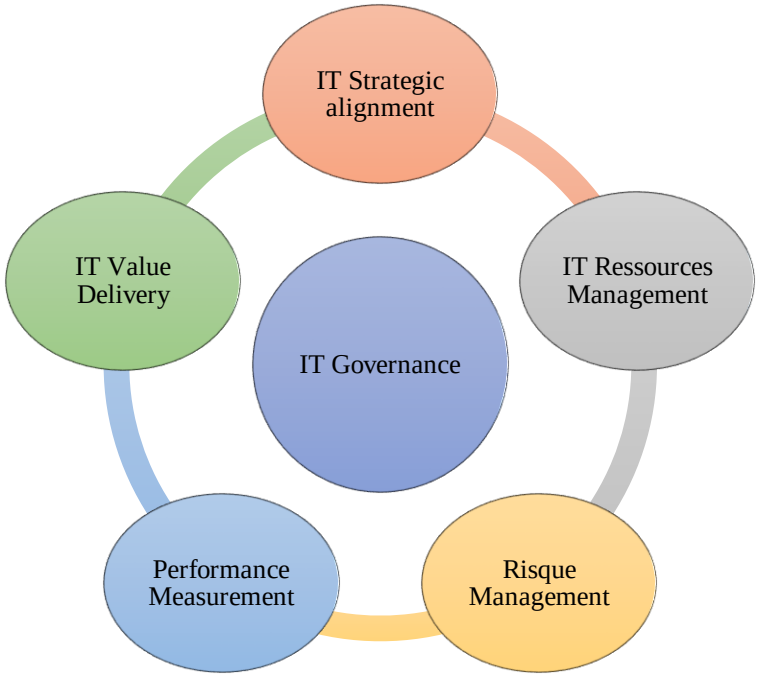
Il n'existe pas de définition commune du terme « Gouvernance IT », L'analyse de la littérature existante a révélé que définir le terme s'avère une tâche difficile en raison de sa nature pluridisciplinaire. Par conséquent, plusieurs chercheurs ont avancé différentes définitions parmi lesquelles on peut mentionner :

- De (Abdelmalek Sadok , al, 2020), qui la décrit comme l'ensemble des structures et processus de leadership et d'organisation visant à aligner l'informatique de l'organisation avec sa stratégie et ses objectifs.
- Selon (ITGI, 2006), la gouvernance des technologies de l'information (IT) est définie comme la responsabilité du conseil d'administration et de la direction générale. Elle englobe le leadership ainsi que les structures et processus organisationnels qui assurent que les technologies de l'information de l'organisation soutiennent et favorisent la réalisation des stratégies et des objectifs de l'entreprise.

En outre la gouvernance des IT englobe les structures, les processus de leadership, les mécanismes de responsabilité ainsi que les méthodes organisationnelles qui sont instaurés au sein d'une entreprise afin d'assurer l'alignement des activités informatiques sur la stratégie et les objectifs globaux de l'entreprise. Elle implique la responsabilité du conseil d'administration et de la direction générale dans la supervision et la gestion des technologies de l'information, tout en établissant des structures et des processus pour garantir que les IT soutiennent efficacement la réalisation des objectifs commerciaux de l'organisation.

L'analyse exhaustive des recherches antérieures dans la littérature révèle que la gouvernance IT repose principalement sur cinq composantes fondamentales :

Figure 3: Les cinq axes de la gouvernance IT



Source : (Uky Yudatama, Bobby Nazief, Achmad Nizar Hidayanto, 2017)

- **Alignement Stratégique des IT (IT Strategic Alignment) :** Cela concerne l'alignement des objectifs et des activités des IT avec la stratégie et les objectifs de l'entreprise pour soutenir sa mission et sa vision.
- **Gestion des Ressources Informatiques (IT Resource Management) :** Cela implique la gestion efficace des ressources IT, y compris les infrastructures, les applications, et le personnel, pour optimiser leur utilisation et leur contribution à la valeur ajoutée de l'entreprise.
- **Gestion des Risques (Risk Management) :** Cela fait référence à l'identification, l'évaluation, et la gestion des risques IT pour minimiser les impacts négatifs sur l'entreprise.
- **Mesure de la Performance (Performance Measurement) :** Cela implique le suivi et l'évaluation des performances des IT pour s'assurer qu'elles atteignent les objectifs fixés et apportent une valeur ajoutée.

- **Livraison de la Valeur des IT (IT Value Delivery) :** Cela se concentre sur la garantie que les investissements IT génèrent une valeur optimale pour l'entreprise, en termes de soutien aux processus métier et d'atteinte des résultats souhaités.

2.2.1.3 Importance de la gouvernance IT

D'après u (Rimol, 2022)", la gouvernance IT est devenue un élément crucial pour la réussite des entreprises à l'ère numérique. Le rapport souligne que les PDG attendent désormais des DSI qu'ils soient des leaders capables d'aligner les stratégies informatiques sur les objectifs commerciaux et de piloter la transformation numérique de l'organisation.

Le rapport identifie plusieurs facteurs qui contribuent à l'importance croissante de la gouvernance IT :

- **L'augmentation de la complexité des SI/IT:** Les environnements informatiques sont de plus en plus complexes, avec l'adoption de technologies telles que le cloud computing, l'Internet des objets (IoT) et l'intelligence artificielle (IA). Cela rend la gouvernance IT encore plus essentielle pour assurer la gestion efficace de ces technologies et minimiser les risques.
- **L'évolution des cybermenaces:** Les cybermenaces deviennent de plus en plus sophistiquées, ce qui expose les organisations à un risque accru de piratage informatique, de fuites de données et d'autres cyberattaques. Une gouvernance IT efficace est essentielle pour mettre en place des mesures de sécurité adéquates et protéger les données de l'organisation.
- **L'importance croissante de l'analyse des données:** Les données sont devenues un atout stratégique majeur pour les entreprises. Une gouvernance IT efficace permet de garantir la qualité, la sécurité et la disponibilité des données, ce qui est essentiel pour une prise de décision basée sur les données et l'innovation.

Le rapport de (Rimol, 2022) recommande aux entreprises de mettre en place un cadre de gouvernance IT robuste qui comprend les éléments suivants :

- **Une vision claire de la gouvernance IT:** Cette vision doit définir les objectifs de la gouvernance IT et les rôles et responsabilités des différentes parties prenantes.
- **Un processus de prise de décision structuré:** Ce processus doit garantir que les décisions concernant les SI/IT sont prises de manière alignée sur les objectifs stratégiques de l'organisation.

- **Un programme de gestion des risques:** Ce programme doit identifier, évaluer et atténuer les risques liés aux SI/IT.
- **Un cadre de contrôle interne:** Ce cadre doit garantir que les processus et les contrôles informatiques sont efficaces et fiables.
- **Des mesures de performance:** Ces mesures doivent permettre de suivre et d'évaluer l'efficacité de la gouvernance IT.

2.2.1.4 Objectifs de la gouvernance IT

D'après (Howard, 2023), les objectifs clés de la gouvernance IT sont les suivants :

- **Aligner les SI/IT sur les objectifs stratégiques de l'organisation:** La gouvernance IT doit garantir que les investissements en SI/IT sont alignés sur les objectifs stratégiques de l'organisation et contribuent à la création de valeur pour l'entreprise.
- **Gérer les risques liés aux SI/IT:** Les SI/IT sont exposés à divers risques, tels que les cybermenaces, les pannes de système et les erreurs humaines. La gouvernance IT doit permettre d'identifier, d'évaluer et d'atténuer ces risques.
- **Optimiser les coûts des SI/IT:** La gouvernance IT doit contribuer à optimiser les dépenses en SI/IT en veillant à ce que les ressources soient utilisées de manière efficace et efficiente.
- **Améliorer l'efficacité opérationnelle des SI/IT:** La gouvernance IT doit permettre d'améliorer l'efficacité opérationnelle des SI/IT en optimisant les processus et en garantissant la qualité des services informatiques.
- **Favoriser l'innovation grâce aux SI/IT:** La gouvernance IT doit créer un environnement propice à l'innovation en permettant aux entreprises de tirer parti des nouvelles technologies pour développer de nouveaux produits et services.

En plus de ces objectifs clés, Howard identifie également plusieurs autres objectifs importants de la gouvernance IT, tels que :

- **Assurer la conformité aux réglementations:** La gouvernance IT doit garantir que les SI/IT sont conformes aux réglementations en vigueur.
- **Protéger les données de l'organisation:** La gouvernance IT doit permettre de protéger les données de l'organisation contre les fuites et les accès non autorisés.

- **Gérer les changements liés aux SI/IT:** La gouvernance IT doit faciliter la gestion des changements liés aux SI/IT, tels que les mises à niveau de logiciels et les déploiements de nouveaux systèmes.

2.2.2 Les activités de la gouvernance

La gouvernance s'appuie sur 3 activités principales :

Figure 4: activités de la gouvernance

Source : (Morisse, 2019)

Surveiller : Les responsables surveillent les performances en utilisant des systèmes de mesure adaptés et veillent à ce qu'elles correspondent aux plans et aux objectifs de l'entreprise.
Évaluer : Les décideurs évaluent l'utilisation actuelle et future des technologies de l'information en tenant compte de l'évolution technologique, des tendances économiques et sociales, ainsi que des contraintes politiques et légales.
Diriger : Les décideurs délèguent les responsabilités pour la préparation et la mise en œuvre des plans et des directives en matière de technologies de l'information qui définissent les investissements à réaliser dans les projets et les services à fournir. Ils veillent à ce que la stratégie soit communiquée de manière efficace au sein de la direction et du management.

2.2.3 Avantage de gouvernance

D'après le (ISACA, 2020), L'Excellence en Gouvernance des Technologies de l'Information (EGIT) se concentre sur deux piliers fondamentaux : ***la création de valeur*** et ***la gestion des risques liés à la transformation numérique***. Cette approche vise à maximiser les avantages de l'Information et de la Technologie (I&T) tout en minimisant les risques commerciaux associés. Elle se traduit par trois résultats clés :

- **Maximisation des avantages** : L'EGIT cherche à créer de la valeur pour l'entreprise en alignant étroitement les investissements dans l'I&T sur les objectifs stratégiques. Cela implique de maintenir et d'accroître la valeur des investissements existants, tout en éliminant les initiatives qui n'apportent pas suffisamment de valeur. L'accent est mis sur la livraison de services et de solutions informatiques adaptés aux besoins, dans les délais

et le budget impartis, tout en mesurant l'impact financier et non financier de ces investissements.

- **Gestion optimisée des risques** : L'EGIT vise à identifier, évaluer et gérer les risques commerciaux associés à l'I&T. Cela comprend les risques liés à l'utilisation, la propriété, l'exploitation, l'implication et l'adoption de l'I&T dans l'entreprise. Cette gestion des risques est intégrée à l'approche globale de gestion des risques de l'entreprise pour garantir la préservation de la valeur commerciale. Les progrès dans ce domaine sont mesurés pour démontrer l'impact de l'optimisation des risques sur la performance globale de l'entreprise.

- **Optimisation des ressources** : L'EGIT s'assure que les ressources nécessaires sont en place pour exécuter le plan stratégique de l'entreprise de manière efficace. Cela comprend la fourniture d'une infrastructure informatique intégrée et économique, l'introduction de nouvelles technologies selon les besoins de l'entreprise, et le maintien des compétences du personnel informatique. L'exploitation efficace des données et des informations est également une composante essentielle de l'optimisation des ressources.

2.3 Audit IT

2.3.1 Présentation de l'audit IT

L'audit informatique, également connu sous le nom « audit des systèmes d'information », est une démarche réalisée par un intervenant externe et indépendant du service auditée. Son objectif est d'analyser tout ou partie de l'organisation informatique d'une entreprise, d'identifier ses forces et ses faiblesses, et de formuler des recommandations en vue d'améliorer ses performances. En d'autres termes, il vise à évaluer les risques liés aux activités informatiques afin de les réduire et d'optimiser la maîtrise des systèmes d'information. Cette évaluation des risques peut concerner divers domaines tels que les opérations, les finances et la réputation de l'entreprise.

La mise en œuvre d'un audit des systèmes d'information repose sur deux principales caractéristiques :

- ✓ Les évaluations globales d'entités, qui consistent à examiner l'ensemble des activités liées aux systèmes d'informations au sein de l'organisation.

- ✓ Les audits thématiques, qui se concentrent sur des aspects spécifiques de l'informatique au sein de l'entité, tels que la gestion de projet ou la sécurité logique.

Il est important de distinguer l'audit de l'activité de conseil, qui vise à améliorer le fonctionnement et la performance de l'organisation. Ces deux activités doivent être menées par des acteurs différents afin d'éviter tout conflit d'intérêts potentiel.

2.3.2 Typologie

La démarche d'audit informatique est une pratique générale qui s'applique à divers domaines tels que la fonction informatique, les études informatiques, les projets informatiques, l'exploitation, la planification de l'informatique, les réseaux et les télécommunications, la sécurité informatique, les achats informatiques, etc.
Voici un a des principaux types d'audits informatiques :

- Audit de la fonction informatique : Vérifie l'organisation, le pilotage, le positionnement dans la structure, les relations avec les utilisateurs, et les méthodes de travail de la fonction informatique en se basant sur des bonnes pratiques telles que la clarté des structures et des responsabilités, les dispositifs de mesure de l'activité, le niveau des compétences du personnel, etc.

- Audit des études informatiques : Vérifie l'efficacité de l'organisation et de la structure des études informatiques, le pilotage, les activités, les relations avec les utilisateurs, etc., en se basant sur des bonnes pratiques comme l'organisation en équipes, le choix des outils et méthodes, le contrôle des activités, la maintenance des applications, etc.

- Audit de l'exploitation : Vérifie l'efficacité de la gestion des centres de production informatiques en se basant sur des bonnes pratiques telles que la clarté de l'organisation, l'existence d'un système d'information dédié, la mesure de l'efficacité des services, etc.

- Audit des projets informatiques : Vérifie le déroulement logique et efficace des projets informatiques en se basant sur des bonnes pratiques comme l'existence d'une méthodologie de conduite des projets, le respect des étapes du projet, la qualité des études amont, l'importance accordée aux tests, etc.

- Audit des applications opérationnelles : Vérifie le fonctionnement des applications opérationnelles en se basant sur des bonnes pratiques telles que la conformité de l'application, la vérification des dispositifs de contrôle, l'évaluation de la fiabilité des traitements, etc.

- Audit de la sécurité informatique : Vérifie le niveau de risque lié à des défauts de sécurité informatique en se basant sur des objectifs de contrôle comme le repérage des actifs informationnels, l'identification des risques, l'évaluation des menaces, la mesure des impacts, et la définition des parades.

2.3.3 Acteur de l'audit et leur rôle

Selon la norme (ISO19011, 2018) l'audit est généralement un « ménage à trois », il met en présence :

- **Un commanditaire** : le commanditaire de l'audit est l'entité ou la personne qui demande à réaliser un audit. Il peut s'agir de l'entité auditée elle-même ou de toute autre organisation ayant le droit réglementaire ou contractuel de demander un audit.

- **Un audité** : L'audité est l'entité ou la personne soumise à l'audit ou qui fait face à l'équipe d'audit, c'est-à-dire celle qui est examinée ou évaluée dans le cadre du processus d'audit. Cela peut être une organisation, un département, un système, ou même une personne individuelle, en fonction du contexte de l'audit.

- **Une équipe d'audit** : l'équipe d'audit généralement composée d'une ou plusieurs personnes chargées de mener l'audit, éventuellement assistées par des experts techniques.
  - Un auditeur n'est pas un certificateur de compte, un juge, un policier ou bien un inspecteur, un auditeur c'est un professionnel du traitement de l'information qui aide un manager à mieux maitriser ses risques et à fonctionner plus efficacement afin d'atteindre ses objectifs.
  - Un auditeur doit se doté de ces qualités :
    - ✓ Intégrité
    - ✓ Objectivité
    - ✓ Capacité d'écoute

- ✓ Indépendance
- ✓ Compétence
- ✓ Esprit d'équipe

2.3.4 Norme liée à l'audit SI

L'activité de l'audit est menée dans le respect d'un cadre de référence :

- ✓ Elles définissent les principes de base de la pratique de l'audit.
- ✓ Elles sont un cadre de référence.
- ✓ Elles établissent les critères d'appréciation du fonctionnement de l'audit.
- ✓ Elles favorisent l'amélioration des processus organisationnels et des opérations.

Tableau 1: liste des référentiels et normes liés à l'audit SI

Référentiel	Description	Domaines d'application	Niveaux de certification
CMMI (Capability Maturity Model Integration)	Modèle de maturité des capacités pour les développements informatiques	gestion de processus et de la qualité	5 niveaux (de 1 à 5)
ITIL (Information Technology Infrastructure Library)	Bibliothèque de bonnes pratiques pour la gestion de la production informatique	Services informatiques et infrastructure IT	Pas de niveaux de certification
COBIT (Control Objectives for Information and related Technology)	Cadre de référence pour la gouvernance des technologies de l'information et des systèmes d'information	Gouvernance, gestion des risques et contrôle des SI	Pas de niveaux de certification
ISO 2700X	Norme internationale pour la sécurité de l'information	Sécurité des systèmes d'information	Certification unique

Source : nous même

2.3.5 Processus de l’audit

L'audit SI est un processus crucial qui permet d'évaluer la sécurité, la fiabilité, l'efficacité et la conformité des systèmes d'information d'une organisation. Il se déroule en trois phases distinctes: la phase de préparation, la phase sur le terrain et la phase de restitution.

2.3.5.1 Phase de Préparation :

Cette phase initiale est essentielle pour établir les bases solides de l'audit. Elle implique les étapes suivantes:

- **Définition des objectifs:** Déterminer clairement ce que l'audit vise à accomplir et à évaluer. Cela implique de définir les questions clés auxquelles l'audit doit répondre.
- **Délimitation du champ d'application:** Identifier les domaines spécifiques des systèmes d'information qui seront examinés lors de l'audit. Cela peut inclure des systèmes spécifiques, des processus ou des fonctions.
- **Récupération des ressources:** Rassembler les documents pertinents, les outils d'audit et les compétences nécessaires pour mener à bien l'audit. Cela peut inclure l'engagement d'experts externes si nécessaire.
- **Planification logistique:** Définir le calendrier de l'audit, identifier les parties prenantes à impliquer et coordonner les activités avec les différents départements ou entités concernées.

2.3.5.2 Phase sur le terrain :

Au cours de cette phase, l'équipe d'audit met en œuvre le plan élaboré lors de la phase de préparation. Les activités principales comprennent:

- **Collecte de données:** Recueillir des informations auprès de diverses sources, telles que des entretiens avec les employés, des revues de documents, des observations sur place et des analyses de données système.
- **Évaluation de la conformité:** Examiner les systèmes d'information par rapport aux normes, politiques et procédures établies par l'organisation.
- **Identification des non-conformités:** Déterminer les domaines où les systèmes d'information ne respectent pas les exigences définies.

- **Reconnaissance des forces:** Identifier les aspects positifs des systèmes d'information et les pratiques exemplaires qui peuvent être partagées.
- **Découverte d'opportunités d'amélioration:** Suggérer des moyens d'améliorer l'efficacité, la sécurité et la gouvernance des systèmes d'information.

2.3.5.3 Phase de Restitution :

La phase finale consiste à communiquer les résultats de l'audit aux parties prenantes concernées. Les étapes clés comprennent:

- **Analyse des données:** Examiner et synthétiser les informations recueillies lors de la phase sur le terrain.
- **Formulation des conclusions:** Déterminer les conclusions principales sur l'état des systèmes d'information et leur conformité aux exigences.
- **Élaboration de recommandations:** Proposer des actions correctives et des mesures d'amélioration pour remédier aux non-conformités et optimiser les systèmes d'information.
- **Présentation des résultats:** Communiquer les conclusions et recommandations aux parties prenantes lors de réunions de restitution formelles.
- **Rédaction du rapport d'audit:** Documenter les résultats de l'audit, les conclusions, les recommandations et les plans d'action convenus.

2.4 Gestion des risques

2.4.1 Définition

2.4.1.1 Le risque

(AFNOR, 2016)**:** « l'effet de l'incertitude sur des objectifs ». En d'autres termes, il s'agit d'un événement potentiel qui peut avoir un impact négatif sur une organisation ou un projet. Le risque est caractérisé par deux éléments principaux :

La probabilité d'occurrence : C'est la chance qu'un événement donné se produise.

La gravité des conséquences : C'est l'ampleur des dommages potentiels que l'événement pourrait causer.

(ISO31000:2018, 2018) **:** « l'expression de l'incertitude quant à l'apparition d'un événement pouvant avoir un impact sur un objectif ». Cette définition met l'accent sur le fait que le risque est lié à l'incertitude. Cela signifie qu'il n'est pas toujours possible de prédire avec certitude si un événement donné se produira ou non, ni quelles seront ses conséquences.
: « Le risque est la menace qu'un événement, une action, ou une inaction affecte la capacité de l'entreprise à atteindre ses objectifs stratégiques et compromette la création de valeur ».

2.4.1.2 Gestion des risques

(AFNOR, 2016)**:** « l'ensemble des activités coordonnées visant à diriger et à contrôler les risques ». En d'autres termes, il s'agit d'un processus systématique qui permet d'identifier, d'analyser, d'évaluer et de traiter les risques afin de minimiser leur impact négatif.

(ISO31000:2018, 2018)**:** « l'application de principes, de méthodes et d'outils à des activités de communication, de consultation et de prise de décision formelles et informelles visant à identifier, analyser, évaluer, traiter, surveiller, communiquer et documenter les risques ». Cette définition met l'accent sur le fait que la gestion des risques est un processus continu et itératif. Cela signifie qu'il est important de revoir et de mettre à jour les plans de gestion des risques régulièrement afin de tenir compte des changements de l'environnement et des nouvelles informations.

(Ernst&young, 2022)**:** « Un processus continu et intégré qui vise à aider les organisations à identifier, évaluer, mettre en œuvre, surveiller les risques potentiels qui pourraient nuire à leurs objectifs stratégiques, opérationnels ou financiers ».

La gestion des risques peut être définie par l'équation suivante :

Risque = (Menace x Vulnérabilité) / Contre-mesures

- **Menace :**

La menace est un événement potentiel qui pourrait causer un dommage à un actif. Il peut s'agir d'une action délibérée, telle qu'une attaque de pirate informatique, ou d'un événement accidentel, tel qu'une catastrophe naturelle.

- **Vulnérabilité :**

La vulnérabilité est une faiblesse d'un système ou d'un actif qui peut être exploitée par une menace. Par exemple, une vulnérabilité logicielle peut permettre à un pirate informatique de prendre le contrôle d'un ordinateur.

- **Contre-mesures :**

Les contre-mesures sont les mesures prises pour réduire le risque d'une menace. Elles peuvent inclure des mesures techniques, telles que l'installation de logiciels de sécurité, ou des mesures organisationnelles, telles que la formation des employés.

Calcul du risque

La formule calcule le risque en divisant le produit de la menace et de la vulnérabilité par les contre-mesures. Cela signifie que :

- Un risque élevé est associé à une menace élevée et à une vulnérabilité élevée, et à de faibles contre-mesures.
- Un risque faible est associé à une menace faible ou à une vulnérabilité faible, ou à des contre-mesures fortes.

2.4.2 Principes de la gestion des risques

L'identification des actifs est la première étape dans le processus de gestion des risques. Cette étape consiste à recenser tous les actifs de l'organisation, qu'ils soient liés aux affaires (business) ou au système (system), qui doivent être protégés. Ces actifs peuvent inclure des données sensibles, des infrastructures informatiques, des équipements, des logiciels, etc.

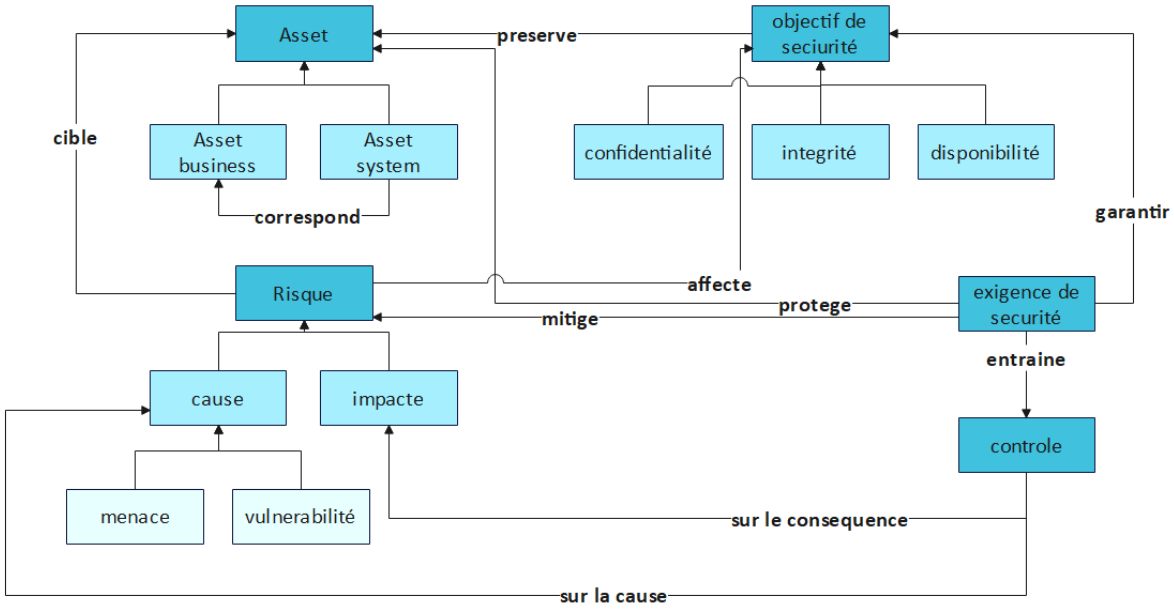
Une fois les actifs identifiés, des objectifs de sécurité spécifiques leur sont associés. Ces objectifs de sécurité visent généralement à préserver la confidentialité, l'intégrité et la disponibilité des actifs et à garantir le respect des exigences de sécurités.

Le risque est ensuite évalué en identifiant ses causes et donc les menaces potentielles qui pourraient affecter les actifs, ainsi que les vulnérabilités qui pourraient être exploitées par ces menaces et son impacte.

Les menaces peuvent inclure des cyberattaques, des catastrophes naturelles, des erreurs humaines, etc., tandis que les vulnérabilités sont des faiblesses ou des lacunes dans les systèmes ou les processus qui pourraient être exploitées par les menaces.

Pour gérer le risque, des contrôles spécifiques sont mis en place en fonction de l'analyse des menaces et des vulnérabilités. Ces contrôles peuvent inclure des mesures de sécurité techniques, telles que des pares-feux et des antivirus, des procédures opérationnelles, telles que des politiques d'accès et de sauvegarde des données, ainsi que des mesures organisationnelles, telles que la sensibilisation à la sécurité et la formation du personnel.

Figure 5: Processus de Gestion des Risques et Sécurité dans un Système d'Information



source : (cHamzaoui, Mohamed, 2008)

2.4.3 Les avantages de la gestion des risques liés aux systèmes d'information

- Elle aide les organisations à prendre des décisions rationnelles concernant la sécurité de leur système d'information.

- La gouvernance des risques du SI protège la technologie et l'infrastructure physique des systèmes, favorisant ainsi la croissance de l'activité et la création de valeur.

- Elle permet de freiner la détérioration et l'utilisation anormale des systèmes et réseaux.

- Elle détecte toute atteinte à l'intégrité, la disponibilité et la confidentialité des informations, limite les conséquences de ces atteintes et, si nécessaire, permet de poursuivre l'auteur du délit.

Les travaux de Westerman et Hunter démontrent qu'une association efficace des volets de gestion du risque, des processus de gouvernance et de la culture de prise en compte des risques permet d'améliorer la performance opérationnelle informatique et métier. Cela offre plusieurs avantages :

- Répondre aux défis posés par les sensibilisations insuffisantes et les lacunes en personnel formé ou en outils pour la gestion du risque.

- Améliorer les performances informatiques en matière de prévention des incidents, d'accompagnement de l'évolution de l'entreprise et d'alignement des objectifs informatiques et métier grâce à une équipe informatique efficace.

- Éviter les risques financiers associés tels que la détérioration de la réputation, la dévaluation des actions, la diminution des ventes, de la productivité et des avantages compétitifs.

2.4.4 Risques opérationnels liés aux systèmes d'information (SI) :

Cela est étudié dans l'étude (IIA, 2015), met en lumière les défis complexes auxquels les organisations sont confrontées dans la gestion des risques opérationnels liés aux SI. À travers des entretiens avec des responsables de l'audit interne et des experts en SI du monde entier il a été conclu que l'ordre de priorité de ces risques peut varier selon le secteur d'activité.

Cybersécurité : Considéré comme le plus significatif par 82% des experts SI, le vol d'informations sensibles par intrusion est pris très au sérieux en raison de ses conséquences sur l'image de marque et la réputation.

Protection des données : La protection des données, en termes de confidentialité, d'intégrité et d'accès, nécessite désormais une approche à plusieurs niveaux pilotée par le responsable de la sécurité des SI.

Projets SI : Les risques associés aux projets SI comprennent le non-respect des délais et du budget, les logiciels défaillants, la moindre efficience et intégration par rapport au plan initial, et le manque de leadership.

Gouvernance des SI : La gouvernance des SI assure que les technologies de l'information soutiennent la stratégie et les objectifs de l'organisation, en prévoyant notamment des dispositifs de contrôle et de reddition de comptes.

Prestation informatique externalisée : L'externalisation expose à des risques, nécessitant une attention particulière aux contrats initiaux et à la supervision continue.

Utilisation des réseaux sociaux : Les organisations doivent définir des politiques pour éviter les risques juridiques, les fuites d'informations et les atteintes à la réputation associés à l'utilisation des réseaux sociaux.

Informatique mobile : Les risques liés à l'informatique mobile incluent la sécurité, la conformité, la protection de la vie privée et la gestion de la flotte d'appareils.

Compétences des auditeurs internes en matière de SI : Un faible nombre d'auditeurs compétents en SI est souvent observé, nécessitant une formation adéquate et une accréditation par la direction des SI.

Technologies émergentes : L'évolution des SI introduit de nouveaux risques, notamment avec l'adoption de technologies émergentes comme le Big Data.

Sensibilisation du conseil et du comité d'audit aux enjeux SI : Les SI nécessitent un investissement majeur et il est crucial que le conseil possède une expertise suffisante pour évaluer leur performance.

2.4.5 Outils et méthodes d'analyse des risques

La gestion des risques liés aux systèmes d'information (SI) est complexe et nécessite une compréhension approfondie des concepts et des processus. Plus de 200 méthodes de gestion et d'analyse des risques sont disponibles, ce qui rend le choix de la méthode appropriée difficile pour les organisations.
Les entreprises recourent à diverses méthodologies et outils spécifiques pour organiser et formaliser leur approche de gestion des risques. La littérature abonde en une multitude de méthodologies, chacune présentant ses propres limitations, aucune n'étant prête à l'emploi. Chaque organisation adapte ces outils à ses besoins, tandis que certaines privilégient même le développement de méthodologies personnalisées, conçues en interne.

Parmi les méthodes les plus utilisées, on trouve EBIOS, OCTAVE et MEHARI. EBIOS, développée par la DCSSI, se concentre sur l'expression des besoins en matière de sécurité et l'identification des objectifs. OCTAVE, créée par le SEI, se démarque par son utilisation des ressources internes de l'organisation pour évaluer les menaces et les vulnérabilités. Quant à

MEHARI, maintenue par le CLUSIF, elle propose une approche holistique de l'analyse des risques, couvrant à la fois les aspects stratégiques et opérationnels.

En ce qui concerne les référentiels normatifs, COSO et COBIT sont largement reconnus. COSO, développé par le Committee Of Sponsoring Organizations, propose un cadre de référence pour le management des risques d'entreprise, tandis que COBIT, publié par l'ISACA, se concentre sur l'évaluation des services informatiques au sein de l'organisation.

Par ailleurs divers outils de gestion des risques sont disponibles et leur utilisation dépend de la nature des projets. Parmi ces outils, on retrouve VPN (Virtual Private Network) qui est une technologie qui crée un tunnel sécurisé entre un appareil et un réseau privé, permettant ainsi de naviguer sur Internet de manière sécurisée et anonyme, en protégeant les données des utilisateurs et en assurant la confidentialité et l'intégrité des informations échangées. En complément, systèmes de suivi des problèmes et des bugs (Bug Track de Symantec) est une plateforme de suivi des problèmes qui permet aux équipes de développement de logiciels de suivre, prioriser et résoudre les bogues signalés. Continuity Planning Tool est un outil vital pour élaborer et gérer les plans de continuité des activités, aidant à identifier les menaces potentielles et à élaborer des stratégies pour maintenir ou rétablir les opérations en cas d'incident majeur. Quant à Nessus, il s'agit d'un scanner de vulnérabilités largement utilisé pour évaluer la sécurité des réseaux informatiques en détectant les vulnérabilités potentielles et en fournissant des rapports détaillés pour permettre des mesures correctives.

Voici quelques méthodes, outils et référentiels liés à la gestion des risques organisés dans un tableau :

Tableau 2: Quelques outils et référentiels liés à la gestion des risques

Méthodes	Outils	Référentiels
EBIOS (Expression des Besoins et Identifications des Objectifs de Sécurité)	**Bug Track de Symantec**	**COSO**
OCTAVE	**Continuity Plan**	**COBIT**
MEHARI (Méthode harmonisée d'analyse des risques)	**Nessus**	
MARION (Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux)	**VPN** (Virtual Private Network)	

(Elaboré par nous meme)

Dans un article détaillant une grille d'évaluation des méthodes d'analyse des risques, (Leger, 2015) observe que CRAMM, EBIOS et Octave semblent être les plus efficaces contrairement à Méhari qui nécessite un encadrement spécifique. Quant aux autres méthodes, elles sont jugées soit immatures, soit difficiles à vérifier.

2.4.6 Processus

La norme (ISO31000:2018, 2018) fournit un cadre structuré pour identifier, analyser et gérer les risques menaçant votre organisation. Afin de rendre ce processus plus accessible, voici une explication simplifiée des étapes clés :

2.4.6.1 Dialogue et concertation : Briser le silence sur les risques

- Initier une communication ouverte et transparente avec toutes les parties prenantes concernées.
- Sensibilisez ces parties prenantes aux risques potentiels auxquels l'organisation est confrontée.
- Encourager l'échange d'informations et la collaboration pour une meilleure compréhension collective des risques.
- Recueillir les avis, les connaissances et les perceptions des parties prenantes afin d'enrichir l'analyse des risques.

2.4.6.2 Poser les jalons : Définir le contexte de votre organisation

- Examiner et analyser l'environnement interne et externe de l'organisation.
- Définir le cadre global dans lequel l'organisation opère afin d'adaptez le processus de gestion des risques en fonction du contexte spécifique de l'organisation.

2.4.6.3 Identification des risques : Détecter les signaux d'alerte

Réaliser une analyse approfondie pour identifier tous les risques potentiels, qu'ils soient internes ou externes.

2.4.6.4 Analyse des risques : Comprendre les tenants et aboutissants

Examiner en détail chaque risque identifié pour en cerner :

- La nature

Inventaire : Biens (Maison, Argent, bijoux,) personnes (famille, ……)

Vulnérabilités : Portes, fenêtre, absence, localisation, …

Menaces : vol, incendies, inondations, ….

- Les causes potentielles
- Les conséquences possibles
- La probabilité d'occurrence.

  L'analyse peut être qualitative ou quantitative, selon les besoins et les ressources de l'organisation.

2.4.6.5 Évaluation des risques : Hiérarchiser les dangers

Pour évaluer les risques, il est crucial de prendre en considération deux aspects principaux :

- La gravité intrinsèque du risque (La potentialité intrinsèque d'un risque), se réfère au niveau maximum des conséquences possibles pour l'organisation sans tenir compte des mesures de sécurité en place.

  Elle dépend de :

  - La localisation et de l'environnement de ce risque
  - De l'enjeu d'un acte volontaire pour son auteur
  - De la probabilité qu'une action volontaire vise précisément l'organisation
- La gravité résiduelle du risque (L'impact intrinsèque), se réfère au niveau maximum des conséquences possibles pour l'organisation en prenant en compte les mesures de sécurité déjà mises en œuvre.

Cela permet d'obtenir une compréhension approfondie des risques, d'évaluer l'efficacité des mesures de sécurité existantes et de hiérarchiser les risques pour une gestion efficace des risques.

L'évaluation du risque se fait en utilisant deux paramètres :

- La probabilité ou la vraisemblance, également connue sous le nom de potentialité.
- L'impact des conséquences, mesurant la gravité des effets.

Cette évaluation permet de classer les risques par ordre de gravité et de priorité pour l'organisation.

2.4.6.6 Traitement des risques : Neutraliser les menaces et saisir les opportunités

- Sélection des options de traitement : Choisir la bonne arme pour chaque bataille
- Sélectionner les actions les plus appropriées pour traiter chaque risque identifié (l'acceptation, la réduction, le transfert ou l'évitement du risque.). Cela doit être adapté aux objectifs, aux ressources et à la tolérance au risque de votre organisation.
- Mise en œuvre des plans d'action : Passer à l'offensive
- Développer des plans d'action détaillés pour mettre en œuvre les mesures de traitement des risques choisies.
- Attribuer les responsabilités et définir des délais clairs pour chaque action.
- Assurer un suivi et un reporting réguliers pour évaluer l'efficacité des actions mises en œuvre.

2.4.6.7 Surveillance et revue : Vigilance et adaptation continues

- Surveiller en permanence l'efficacité des mesures de traitement des risques mises en place.
- Réaliser des revues périodiques du processus de gestion des risques dans son ensemble.
- Tenir compte des changements dans l'environnement interne et externe de l'organisation.
- Évaluer la pertinence des mesures de traitement des risques existantes.
- Apporter les ajustements nécessaires pour maintenir un processus de gestion des risques efficace et adapté.

2.5 MEHARI

(CLUSIF, 2022)

La sécurité du système d'information est cruciale pour toute entreprise, car une défaillance peut entraîner des conséquences désastreuses telles que la détérioration de son image de marque, le vol de ses secrets industriels ou la perte de données critiques, pouvant même mener à sa faillite. Pour garantir cette sécurité, les responsables informatiques disposent de différentes méthodes telles que EBIOS, MEHARI, MARION, MELISA, OCTAVE, etc. Ces méthodes leur fournissent des cadres et des processus pour élaborer une politique de sécurité robuste et réaliser des audits afin d'en vérifier l'efficacité. Organiser la sécurité informatique n'est pas une tâche aisée, mais ces méthodes sont conçues pour faciliter cette démarche et garantir une protection adéquate du système d'information de l'entreprise.

2.5.1 Présentation de MEHARI

M : Management (Gouvernance) : Cet élément souligne l'importance d'une culture et d'une structure de gouvernance solides en matière de gestion des risques.

E : Évaluation (Évaluation) : Cet élément se concentre sur l'identification et l'évaluation des risques.

H : Humain : Cet élément reconnaît l'importance du facteur humain dans la gestion des risques.

A : Analyse (Analyse) : Cet élément met l'accent sur la nécessité d'une approche systématique de l'analyse des risques.

R : Réduction (Réduction) : Cet élément se concentre sur le développement et la mise en œuvre de stratégies de traitement des risques.

I : Amélioration (Amélioration) : Cet élément souligne l'importance de l'amélioration continue du processus de gestion des risques.

MEHARI, développée et entretenue en France par le CLUSIF depuis 1995, est une approche exhaustive pour évaluer et gérer les risques liés à l'information, ses traitements et les ressources associées. Disponible en français et en anglais, MEHARI est issue des méthodes MARION et MELISA, désormais inactives depuis plusieurs années. En tant qu'outil de sécurité des systèmes d'information, MEHARI demeure largement utilisée, offrant une gamme variée d'approches pour appréhender le risque au sein des organisations.

MÉHARI comprend trois bases de connaissances :

- Méhari-Expert : version destinée aux grandes ou très grandes entreprises et nécessitant une bonne expertise de la méthode ;
- Méhari-Standard : version, destinée aux entreprises moyennes ou grandes, dotée de plus d'outils de pilotage et d'accès plus facile ;
- Méhari-ManagerBC : version destinée aux analyses ciblées d'activités ou de projets.

Le CLUSIF, fondé en 1984, est une association française regroupant des entreprises et des collectivités, dédiée au traitement et à l'échange d'informations sur divers aspects de la sécurité de l'information, notamment la gestion des risques, les politiques de sécurité et la cybercriminalité. Les résultats des travaux du CLUSIF, y compris la méthodologie MEHARI, sont accessibles sur son site web.

2.5.2 Objectifs de MEHARI

MEHARI vise principalement à offrir une méthode complète d'analyse et de gestion des risques, en se concentrant spécifiquement sur le domaine de la sécurité de l'information, tout en fournissant tous les outils et moyens nécessaires à sa mise en œuvre. En plus de cet objectif principal, trois autres objectifs viennent s'ajouter :

- ✓ Pas seulement d'identifier les situations de risque et d'en apprécier le niveau, mais de mettre en évidence les mesures permettant de ramener les risques à un niveau acceptable.
- ✓ Faciliter une analyse directe et personnalisée des situations à risque à travers des scénarios détaillés.
- ✓ Offrir une palette complète d'outils adaptés à la gestion de la sécurité à court, moyen et long terme, quel que soit le niveau de maturité de l'organisation en matière de sécurité et les types d'actions envisagés.

2.5.3 Principes de la méthode MEHARI

2.5.3.1 Principe fondamental de MEHARI : Maîtrise totale du risque

Les modules de MEHARI s'appuient sur un pilier central : **ne jamais minimiser un risque**. Cette approche se concrétise par deux principes clés :

- ✓ **Envisager systématiquement les scénarios les plus graves possibles**: Il s'agit d'anticiper les conséquences les plus néfastes qui pourraient découler d'un risque donné, afin de mieux se préparer et d'adopter des mesures adéquates.

- ✓ **Ne considérer que les effets "maîtrisés" des mesures de sécurité**: MEHARI met l'accent sur l'évaluation réaliste de l'efficacité des mesures de sécurité. Seuls les effets avérés et mesurables de ces mesures sont pris en compte, garantissant une approche pragmatique et fiable de la gestion des risques.

2.5.3.2 Un allié puissant pour la sécurité de l'information

MEHARI offre un ensemble d'outils et de ressources précieux pour accompagner les organisations dans la gestion et la sécurisation de leur information. Ce cadre méthodologique complet propose :

Une analyse approfondie des enjeux critiques: MEHARI permet d'identifier et de comprendre les éléments d'information les plus sensibles pour l'organisation, afin de prioriser les efforts de protection.

Un examen méticuleux des vulnérabilités: MEHARI guide l'organisation dans la détection et l'évaluation des failles potentielles de son système d'information, permettant ainsi une prévention ciblée des risques.

Des stratégies efficaces pour atténuer la gravité des risques: MEHARI propose des solutions concrètes pour réduire l'impact potentiel des incidents de sécurité, minimisant ainsi les dommages causés à l'organisation.

Un pilotage éclairé de la sécurité de l'information: MEHARI offre un cadre de gouvernance clair pour la gestion des risques liés à l'information, permettant une prise de décision éclairée et cohérente en matière de sécurité.

2.5.3.3 Flexibilité et adaptabilité : Les atouts de MEHARI

Les modèles de risque MEHARI s'adaptent aux besoins spécifiques de chaque organisation et peuvent être personnalisés en fonction des orientations stratégiques et des politiques de sécurité en vigueur. Cette flexibilité permet d'élaborer des plans d'action pertinents et de faciliter une prise de décision efficace en matière de sécurité de l'information.

2.5.4 Modèle de risque MEHARI : Une approche bi-dimensionnelle

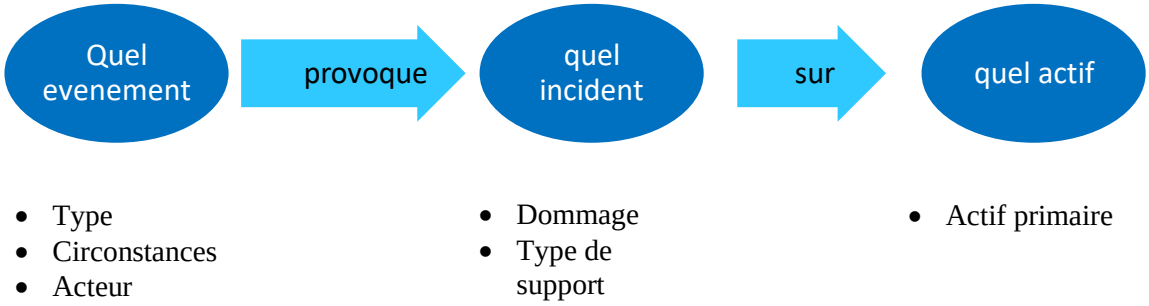
MEHARI s'appuie sur un modèle de risque complet qui combine deux dimensions essentielles :

2.5.4.1 Le modèle de risque qualitatif :

Cette approche permet de cerner les différentes composantes d'un risque et les facteurs qui influencent son niveau de gravité. Elle offre une compréhension fine des enjeux et favorise une évaluation précise des risques.

MEHARI adopte une approche méthodique pour décrire chaque risque, le représentant sous la forme d'un scénario détaillé composé de plusieurs éléments clés. Cette décomposition permet une analyse précise et exhaustive de chaque risque.

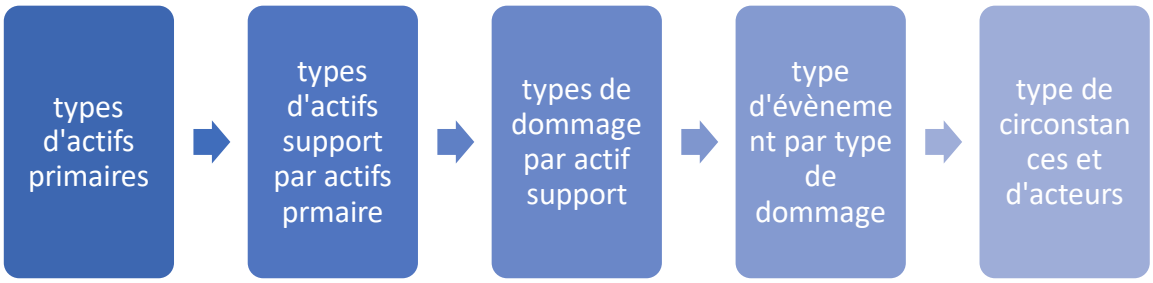
Figure 6: approche méthodique MEHARI



(Méthode Standard - Clusif)

Afin de garantir une standardisation et une exhaustivité dans l'identification des situations de risque, MEHARI définit des typologies spécifiques. Ces typologies servent de cadre pour la description des risques, facilitant ainsi une analyse rigoureuse et cohérente.

Figure 7: Classification des Actifs



(Méthode Standard - Clusif)

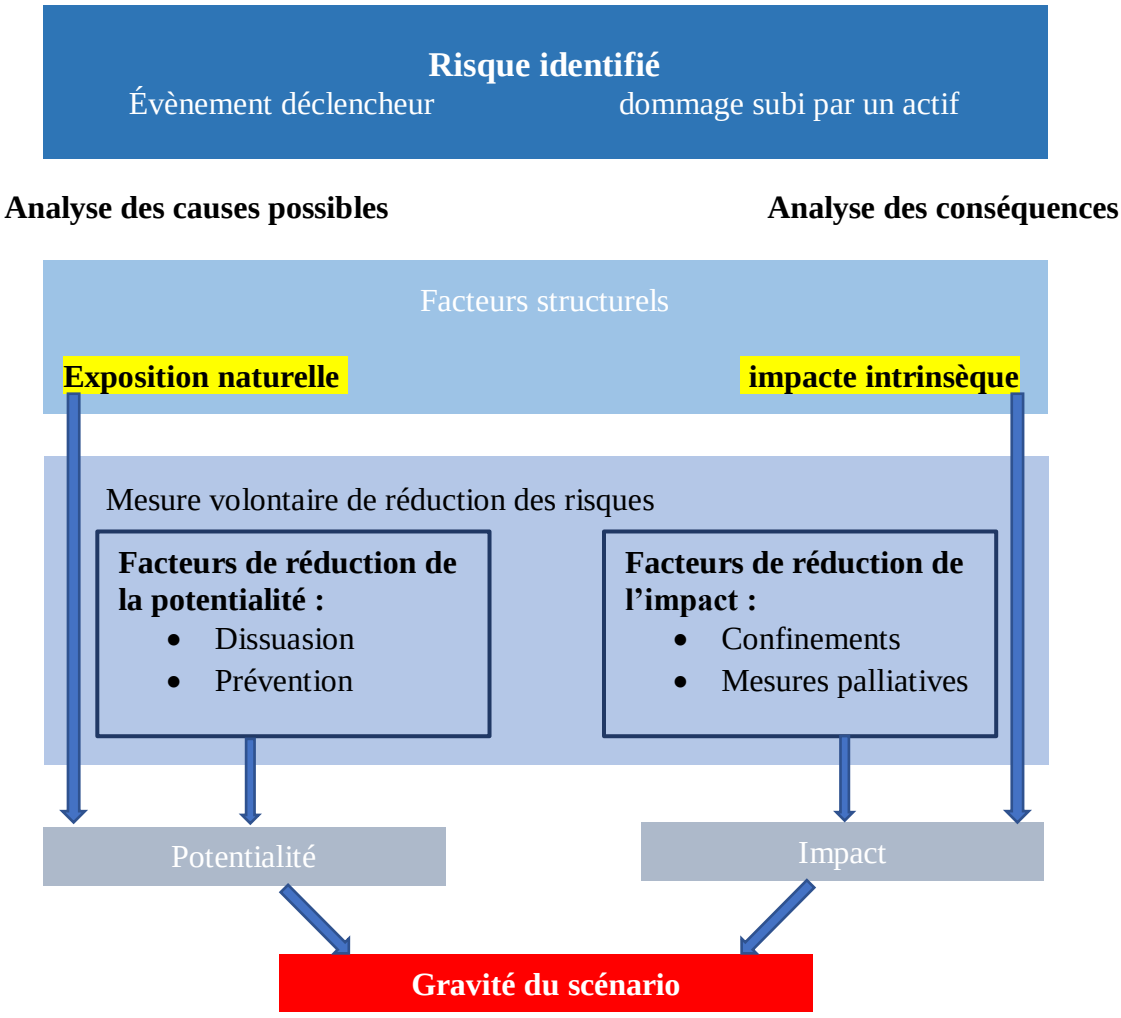
En s'appuyant sur les éléments et typologies décrits précédemment, MEHARI propose une classification des modes d'action possibles pour réduire les risques. Ces modes d'action,

également appelés "Facteurs de réduction de risque", se répartissent en quatre catégories principales :

- **Dissuasion**: Cette approche vise à diminuer la probabilité qu'un acteur malveillant décide de mener l'action à l'origine du risque, en dissuadant son passage à l'acte par des mesures appropriées.
- **Prévention**: Ce mode d'action cherche à rendre plus difficile, voire improbable, la réalisation du risque en mettant en place des mesures qui empêchent le déclenchement de l'événement initial.
- **Confinement**: En cas de survenance du risque, l'objectif du confinement est de limiter l'étendue des dommages directs en mettant en œuvre des solutions de protection et de limitation des dégâts.
- **Palliation**: Cette approche s'active après la réalisation du risque et vise à minimiser les conséquences indirectes des dommages causés. Elle permet de limiter l'impact global du risque sur l'organisation.

Ces modes d'action sont des « Facteurs de réduction de risque ». Le schéma ci-dessous illustre le modèle global de risque qualitatif MEHARI, en mettant en évidence les interactions entre les différents éléments et les modes d'action possibles pour la réduction des risques.

Figure 8: Model global des facteurs de réduction de risque



(Méthode Standard - Clusif)

2.5.4.2 Le modèle de risque quantitatif

Le volet "quantitatif" du modèle de risque MEHARI apporte une dimension chiffrée essentielle à l'analyse des risques, permettant aux organisations de prioriser leurs actions de prévention et de mesurer l'efficacité de leurs stratégies de sécurité. Il se compose de trois éléments clés :

- **Quantification des services de sécurité**: Cette étape vise à définir et à évaluer de manière chiffrée l'efficacité des services de sécurité mis en place pour contrer les risques identifiés. Cela permet d'apprécier leur impact réel sur la réduction des risques.

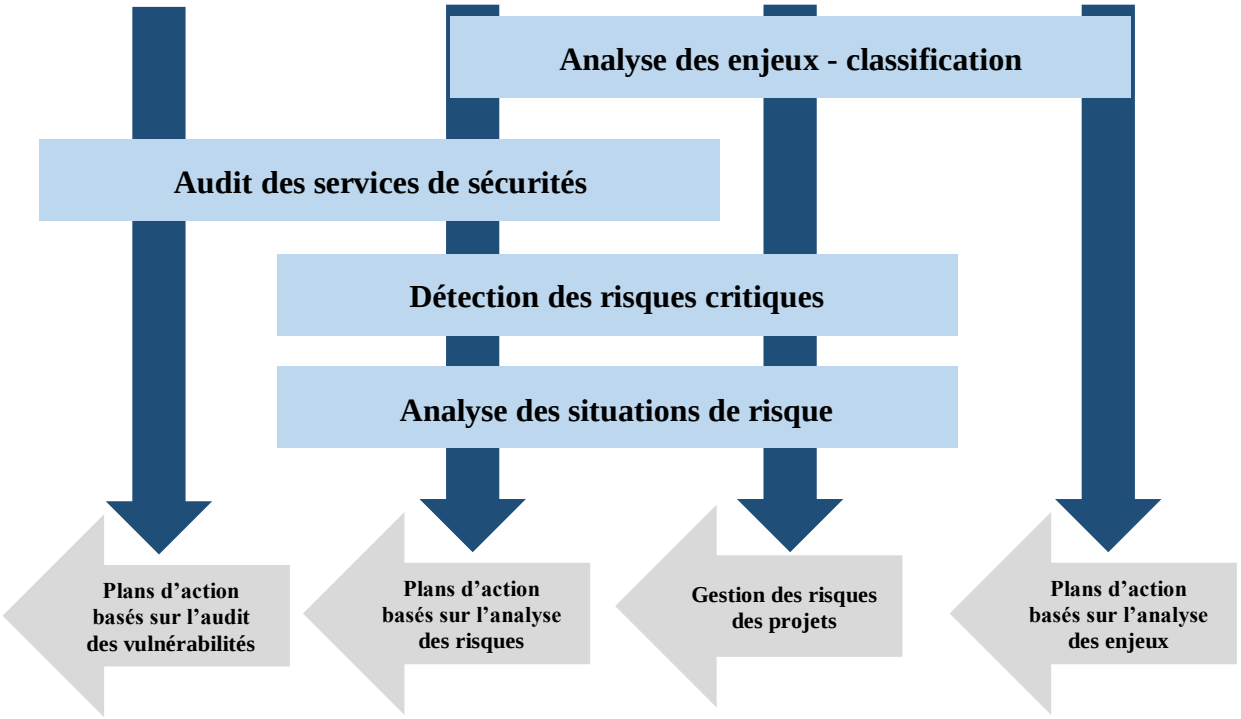
- **Évaluation quantitative des facteurs de réduction de risque**: Pour chaque scénario de risque analysé, MEHARI propose une évaluation quantitative des facteurs de réduction de risque identifiés précédemment. Cette quantification permet de mesurer l'impact précis de chaque facteur sur la réduction du risque global.
- **Évaluation chiffrée du niveau de gravité des risques**: En prenant en compte les effets cumulés des facteurs de réduction de risque, MEHARI permet d'aboutir à une évaluation chiffrée du niveau de gravité de chaque risque. Cette approche quantitative offre une vision claire et objective du niveau de risque résiduel, facilitant ainsi la prise de décision éclairée en matière de gestion des risques.

2.5.5 Processus

La méthode MEHARI, outil précieux pour la gestion des risques informatiques, se décompose en étapes distinctes, chacune jouant un rôle crucial dans l'identification, l'évaluation et la mitigation des risques potentiels.

La figure suivante illustre les étapes de la méthode en mettant en avant ces plans d'action résultants.

Figure 9: Les étapes de la méthode MEHARI



(Méthode Standard - Clusif)

2.5.5.1 Analyse des enjeux : Poser les bases de la protection

L'analyse des enjeux constitue la première étape de la méthode MEHARI. Elle vise à identifier les actifs critiques de l'organisation, qu'il s'agisse de données sensibles, de systèmes informatiques ou d'infrastructures physiques.

Cette étape cruciale permet de définir le périmètre de protection et de prioriser les efforts de sécurisation en fonction de la valeur et de la criticité des actifs identifiés.

- Résultat : Plans d'action initiaux

L'analyse des enjeux génère des plans d'action initiaux qui servent de base pour les étapes ultérieures. Ces plans peuvent inclure des mesures préventives immédiates, telles que la mise en place de sauvegardes régulières ou la sensibilisation des employés aux bonnes pratiques de sécurité.

2.5.5.2 Audit des services de sécurité : Évaluer les défenses existantes

L'audit des services de sécurité s'inscrit comme la deuxième étape de la méthode MEHARI. Il consiste à examiner en profondeur les mesures de sécurité déjà mises en place au sein de l'organisation. Cela inclut l'évaluation des pares-feux, des systèmes de détection d'intrusion, des contrôles d'accès et d'autres mécanismes de protection.

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

L'audit des services de sécurité met en lumière les failles de sécurité existantes et permet de dresser une liste précise des vulnérabilités potentielles. Sur la base de ces résultats, des plans d'action spécifiques sont élaborés pour remédier aux vulnérabilités identifiées et renforcer la posture de sécurité de l'organisation.

2.5.5.3 Détection des risques critiques : Identifier les menaces potentielles

La troisième étape de la méthode MEHARI se concentre sur la détection des risques critiques. Cette étape implique une analyse approfondie des menaces internes et externes auxquelles l'organisation est confrontée. Cela inclut l'évaluation des risques liés aux logiciels malveillants, aux attaques par déni de service, aux intrusions physiques et à d'autres menaces potentielles.

- Résultat : Analyse des situations de risque

L'analyse des situations de risque permet d'identifier les scénarios concrets dans lesquels une vulnérabilité pourrait être exploitée par une menace. Cette analyse précise le niveau de risque encouru par l'organisation et permet de prioriser les actions de mitigation.

2.5.5.4 Plans d'action basés sur l'audit des vulnérabilités :

Cette étape consiste à élaborer des plans d'action spécifiques pour remédier aux vulnérabilités identifiées lors de l'audit des services de sécurité. Cela peut inclure des correctifs logiciels, des mises à jour de sécurité, ou des améliorations des processus.

2.5.5.5 Plans d'action basés sur l'analyse des risques :

De manière similaire, cette étape implique le développement de plans d'action pour traiter les risques identifiés lors de l'analyse des situations de risque. Ces plans peuvent être axés sur la prévention, la mitigation, ou la réponse aux incidents de sécurité.

2.5.5.6 Gestion des risques des projets :

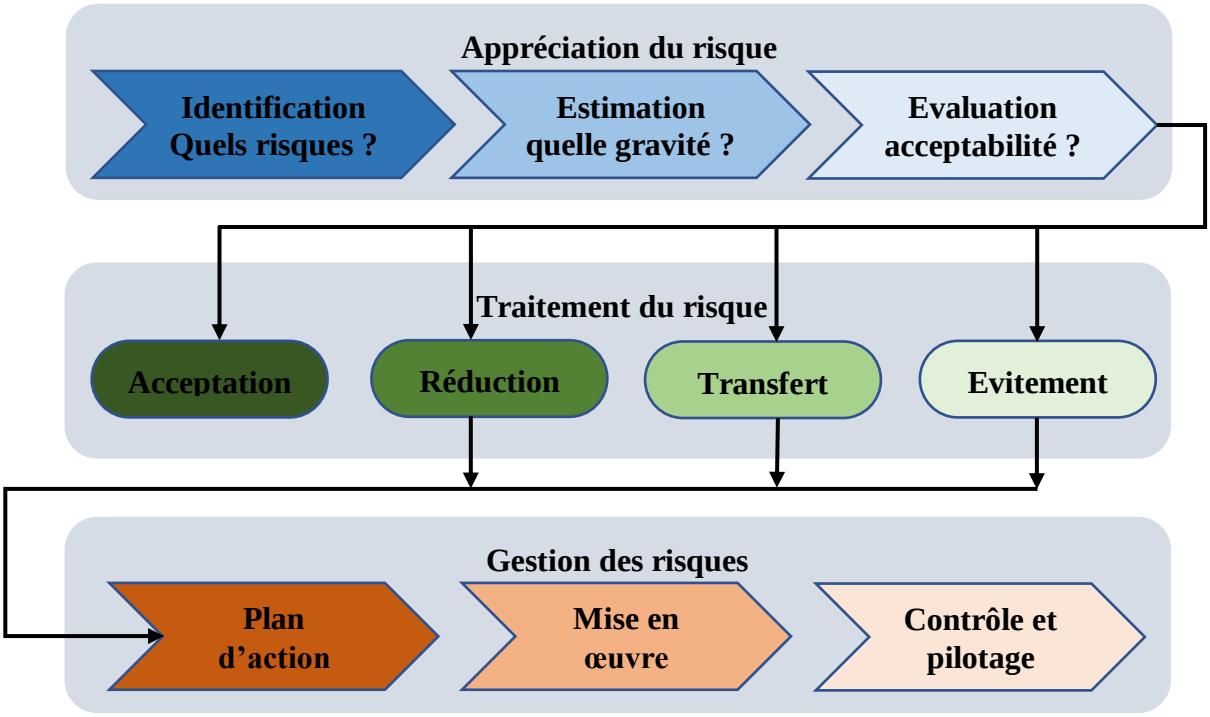
Cette composante s'attache à intégrer la gestion des risques liés à la sécurité dans la planification et l'exécution des projets de l'organisation. Cela garantit que les risques potentiels sont pris en compte dès le début et gérés de manière appropriée tout au long du cycle de vie du projet.

2.5.5.7 Plans d'action basés sur l'analyse des enjeux :

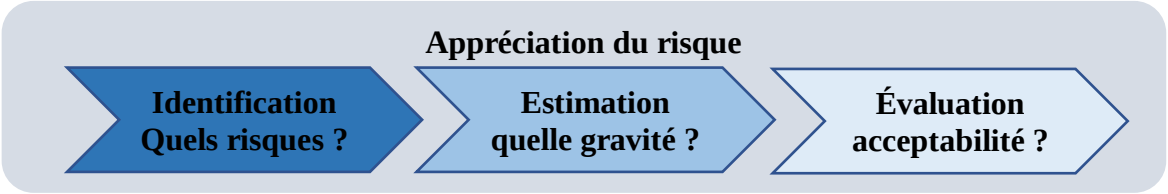
cette partie du processus vise à développer des plans d'action spécifiques pour répondre aux enjeux de sécurité identifiés précédemment. Ces plans peuvent inclure des mesures de sécurité supplémentaires, des formations pour le personnel, ou des investissements dans de nouvelles technologies de sécurité.

2.5.6 Méthodologie

Figure 10: Méthodologie MEHARI



2.5.6.1 Appréciation des risques



2.5.6.1.1 **Identification des risques** :

La première étape consiste à identifier les risques potentiels qui pourraient nuire à un système d'information. Cela implique de rassembler des informations provenant de sources diverses, telles que :

- **Sources internes** : Documentation du système, rapports d'incident, entretiens avec les employés et évaluations des vulnérabilités.
- **Sources externes** : Rapports sectoriels, articles de presse et flux de renseignements sur les menaces.

Les éléments caractéristiques d'un risque sont les suivants :

- **L'actif:** Il s'agit du composant du système d'information qui pourrait être endommagé par le risque.
- **La vulnérabilité intrinsèque:** Il s'agit d'une faiblesse inhérente à l'actif qui pourrait être exploitée par une menace.
- **Le dommage:** Il s'agit des conséquences négatives que le risque pourrait avoir sur l'organisation.
- **La menace:** Il s'agit d'un événement ou d'une situation qui pourrait causer le dommage.
- **Le scénario de risque:** Il s'agit d'une description détaillée du risque, qui comprend tous les éléments caractéristiques mentionnés ci-dessus.

Le processus d'identification des risques MEHARI comprend les étapes suivantes :

1. **Élaboration de la liste des éléments caractéristiques des risques:** Il s'agit de définir les différentes catégories d'éléments caractéristiques des risques, tels que l'actif, le degré de criticité, les types de vulnérabilités, etc.
2. **Élaboration de la liste des risques possibles:** Il s'agit de lister toutes les combinaisons possibles d'éléments caractéristiques des risques.
3. **Développement d'une base de connaissances de risques types:** Il s'agit de créer une base de données qui contient des descriptions de risques types.
4. **Sélection des risques à prendre en compte:** Il s'agit de sélectionner les risques qui sont pertinents pour l'organisation et qui font l'objet de la gestion des risques.

2.5.6.1.2 Estimation de la probabilité et de l'impact des risques :

Paramètres d'estimation des risques

La méthode MEHARI s'appuie sur deux paramètres clés pour évaluer le risque :

1. **Potentialité:** La probabilité ou la vraisemblance qu'un risque se produise. Elle représente la chance que la menace se concrétise.

2. **Impact:** La gravité des conséquences potentielles si le risque se matérialise. Elle représente l'ampleur des dommages que la menace pourrait causer à l'organisation.

Échelles de potentialité et d'impact

MEHARI propose des échelles standardisées à quatre niveaux pour la potentialité et l'impact, permettant une évaluation cohérente et comparative des risques. Ces échelles prennent en compte divers facteurs tels que la nature de la menace, la vulnérabilité des systèmes d'information et les capacités des acteurs malveillants.

Facteurs influençant la potentialité intrinsèque

La potentialité intrinsèque d'un risque dépend de plusieurs facteurs :

- **Localisation et environnement du risque:** Le contexte dans lequel le risque se présente peut influencer sa probabilité d'occurrence.
- **Enjeu d'un acte volontaire:** La motivation des acteurs malveillants à exploiter une vulnérabilité est un élément important à considérer.
- **Probabilité d'une action ciblée:** La probabilité qu'une attaque soit spécifiquement dirigée contre l'organisation joue un rôle dans l'évaluation du risque.

Facteurs influençant l'impact intrinsèque

L'impact intrinsèque d'un risque dépend également de plusieurs facteurs :

- **Sensibilité des actifs informationnels:** La criticité des données et des systèmes d'information exposés à la menace détermine la gravité potentielle des conséquences.
- **Criticité des processus métier:** L'impact potentiel sur les opérations commerciales et la continuité d'activité est un facteur crucial à évaluer.
- **Pertes financières potentielles:** Les dommages financiers directs et indirects encourus en cas de matérialisation du risque doivent être pris en compte.
- **Atteinte à la réputation:** Les conséquences négatives sur l'image et la crédibilité de l'organisation ne doivent pas être négligées.

Impact des mesures de sécurité

Les mesures de sécurité jouent un rôle essentiel dans la réduction des risques en influençant à la fois la potentialité et l'impact.

Facteurs de réduction de la potentialité:

- **Mesures cumulatives:** Empêcher la survenance de l'événement, comme des barrières physiques ou des contrôles d'accès.

- **Mesures de dissuasion:** Décourager les acteurs de la menace de lancer une attaque, comme une présence de sécurité visible ou des politiques de dissuasion.

- **Mesures de prévention:** Entraver la réussite d'une attaque, comme le cryptage, les systèmes de détection d'intrusion ou les pares-feux.

Facteurs de réduction de l'impact:

- **Mesures cumulatives:** Limiter les conséquences directes d'une attaque, comme des plans de reprise d'activité après sinistre ou des procédures de sauvegarde.

- **Mesures de confinement:** Limiter la propagation des dommages, comme la segmentation des données ou la segmentation du réseau.

- **Mesures d'atténuation:** Minimiser les conséquences indirectes, comme les plans de continuité des activités ou les stratégies de gestion de la réputation.

Processus d'estimation des risques :

Comprend deux phases distinctes : stratégique et opérationnelle.

1. Élaboration des éléments de référence :

- Définition des échelles d'impact, de potentialité et des niveaux des facteurs de réduction des risques.
- Objectif : hiérarchiser les niveaux de conséquences, de probabilité et d'efficacité des mesures de sécurité.

2. Évaluation des risques :

- Évaluation de l'impact et de la potentialité intrinsèques. (À faire en se basant sur les définitions de niveaux et en faisant abstraction de toute mesure de sécurité.)
- Évaluation des facteurs de réduction des risques.
    - Recherche des mesures de sécurité pertinentes pour chaque scénario de risque.
    - Détermination des effets des mesures et des niveaux correspondants.
    - Fixation du niveau de chaque facteur de réduction de risque en se référant aux niveaux maximums atteints par les mesures pertinentes.

3. Évaluation de l'impact et de la potentialité résiduels des risques :

- Basée sur les évaluations intrinsèques et des facteurs de réduction des risques.
- Utilisation de grilles de décision pour rendre les jugements reproductibles, en fonction du type de scénario de risque.

2.5.6.1.3 Évaluation de l'acceptabilité des risques :

La dernière étape de l'estimation des risques consiste à évaluer l'acceptabilité de chaque risque. Cela signifie décider si le risque est tolérable ou s'il doit être traité d'une manière quelconque.

Plusieurs facteurs doivent être pris en compte lors de l'évaluation de l'acceptabilité d'un risque, tels que :

- L'impact financier potentiel du risque.
- L'impact potentiel sur la réputation de l'organisation.
- La disponibilité de contrôles pour atténuer le risque.
- La tolérance au risque de l'organisation.

La méthode MEHARI, qui propose une méthodologie complète d'évaluation et de gestion des risques, classe les risques en trois catégories en fonction de leur gravité globale :

- **Risques intolérables** (Niveau de gravité 4) : Il s'agit de risques qui présentent une menace inacceptable pour l'organisation et qui nécessitent une action immédiate. Ils exigent des mesures d'atténuation urgentes pour prévenir ou minimiser les dommages potentiels.
- **Risques inadmissibles** (Niveau de gravité 3) : Ces risques sont considérés comme des menaces importantes qui doivent être éliminés ou réduits dans un délai défini. Ils justifient une attention immédiate et des plans de traitement des risques priorisés pour les ramener à un niveau acceptable.
- **Risques tolérés** (Niveaux de gravité 1 et 2) : Ces risques sont jugés gérables et peuvent être acceptés dans le cadre de la tolérance au risque de l'organisation. Toutefois, ils nécessitent toujours une surveillance continue et des mesures d'atténuation potentielles pour garantir qu'ils restent dans des limites acceptables.

Déterminer la gravité du risque

Pour classer un risque dans l'une de ces catégories, MEHARI utilise un processus en deux étapes :

1. Calculer la probabilité du risque :

Évaluer la probabilité que le risque se produise, en tenant compte de facteurs tels que les données historiques, les tendances du secteur et les évaluations de vulnérabilité. Attribuer un score de probabilité compris entre 1 (très faible) et 5 (très élevé).

2. Matrice de gravité des risques :

Déterminer les conséquences potentielles de la matérialisation du risque, en tenant compte de facteurs tels que les pertes financières, les atteintes à la réputation et les perturbations opérationnelles. Attribuer un score d'impact compris entre 1 (très faible) et 5 (très élevé).

Matrice de gravité des risques

MEHARI utilise une matrice de gravité des risques qui combine les scores de probabilité et d'impact pour déterminer le niveau global de gravité du risque :

Figure 11: Matrice gravité impact probabilité

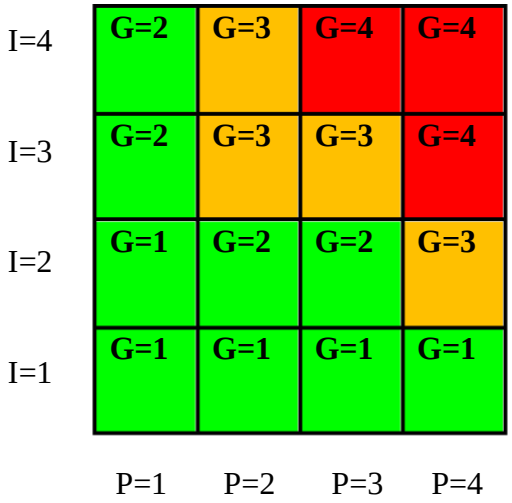


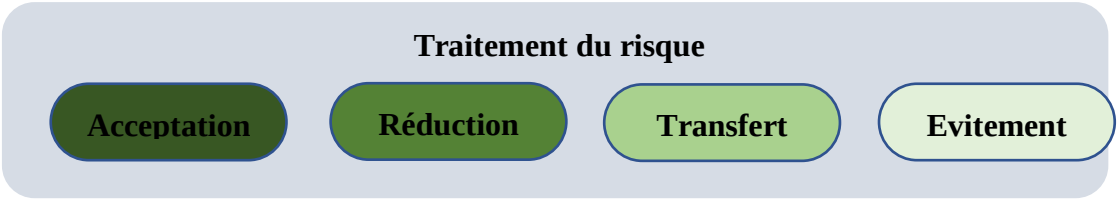
Tableau 3: Les niveaux de gravité

Niveau de gravité	Décision
Intolérable (4)	Rejeter le risque ou mettre en œuvre des mesures d'atténuation immédiates
Inadmissible (3)	Élaborer un plan de traitement des risques avec des délais définis pour la réduction des risques
Tolérable (1 & 2)	Surveiller le risque et mettre en œuvre des mesures préventives si nécessaire

2.5.6.2 Traitement des risques

Une fois les risques identifié et évalués, l'étape suivante consiste à décider comment les traiter. Cela implique de sélectionner l'option de traitement la plus appropriée pour chaque risque et de développer un plan pour mettre en œuvre cette option.

Et pour cela, MEHARI propose quatre stratégies pour traiter les risques identifiés :



2.5.6.2.1 Accepter

Définition: la décision d'accepter un risque est généralement prise lorsque le risque est jugé tolérable ou lorsqu'il n'existe pas d'options d'atténuation réalisables ou rentables.

Quand accepter un risque ?

- le risque a été évalué comme tolérable dans la « grille d'acceptabilité des risques » ;
- pour des raisons économiques (ou autre) , il a été jugé impossible d'y trouver une solution.

2.5.6.2.2 Réduire

Définition: Sélectionner des services de sécurité à partir d'une "base de connaissances" implique :

- Identifier chaque service avec sa finalité ou son objectif spécifique.
- Détailler les mécanismes techniques et organisationnels nécessaires à sa mise en œuvre efficace.
- Évaluer chaque service selon un niveau de qualité prédéfini, afin de :

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

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

Quand réduire un risque ?

- Le risque est inacceptable mais peut être atténué par des mesures rentables.
- Il existe des options d'atténuation efficaces.
- Les avantages potentiels de l'atténuation l'emportent sur les coûts.

2.5.6.2.3 Transférer

Définition: Le transfert de risque consiste à déplacer la charge financière d'un risque vers une autre partie. Cela peut se faire par le biais d'une assurance, d'une externalisation ou d'autres accords contractuels.

Quand transférer un risque ?

- Le risque est trop important pour que l'organisation puisse le supporter seule.
- Il existe un tiers disposé et capable d'accepter le risque.
- Le coût du transfert de risque est inférieur au coût potentiel du risque.

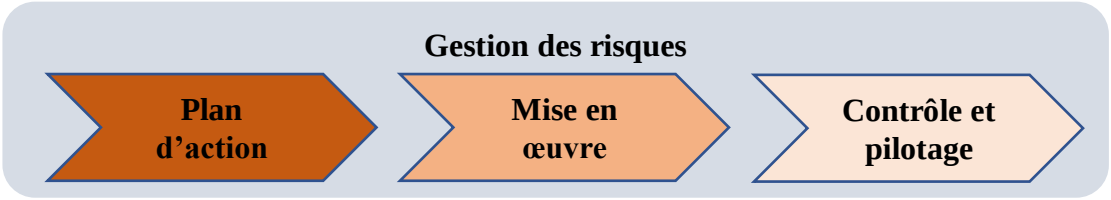
2.5.6.2.4 Éviter

Définition: L'évitement des risques consiste à éliminer complètement le risque en changeant le plan d'action ou l'activité commerciale. Cela peut être un moyen très efficace de gérer les risques, mais cela peut aussi être l'option la plus difficile et la plus coûteuse.

Quand éviter un risque ?

- Le risque est inacceptable et ne peut être atténué ou transféré.
- Les coûts d'évitement sont compensés par les avantages.
- Il existe une alternative claire et viable à l'activité à risque.

2.5.6.3 Gestion des risques



La gestion des risques intervient après avoir pris des décisions concernant le traitement des risques. Elle englobe l'ensemble des processus nécessaires pour mettre en œuvre ces décisions, contrôler leurs effets et les améliorer si nécessaire.

L'élaboration des plans d'action comprend plusieurs étapes :

1. Mise en place des services de sécurité, chacun ayant un objectif de niveau de qualité spécifique.
2. Mise en œuvre de mesures structurelles pour réduire l'exposition à certains risques.
3. Adoption de mesures organisationnelles pour éviter certains risques.

Cependant, en raison de contraintes budgétaires ou de personnel, toutes ces actions ne peuvent pas être entreprises simultanément. Il est donc nécessaire de définir des priorités et d'optimiser les choix. Pour ce faire, plusieurs facteurs sont pris en compte, notamment :

- Les niveaux de gravité des risques à traiter en premier.
- Le nombre de risques à traiter immédiatement par rapport à ceux pouvant être reportés.
- La rapidité avec laquelle des résultats peuvent être observés.
- L'impact sur la sensibilisation du personnel, entre autres.

1. Choix des objectifs prioritaires et optimisation : Pour définir les priorités, il est essentiel de prendre en compte plusieurs facteurs, notamment :

- Les niveaux de gravité des risques que les mesures prioritaires permettront de réduire. Les risques les plus élevés doivent être traités en premier.
- Le nombre de risques traités immédiatement et ceux dont le traitement sera différé.

- La rapidité avec laquelle les premiers résultats pourront être observés.
- L'impact de ces choix sur la sensibilisation du personnel, entre autres.

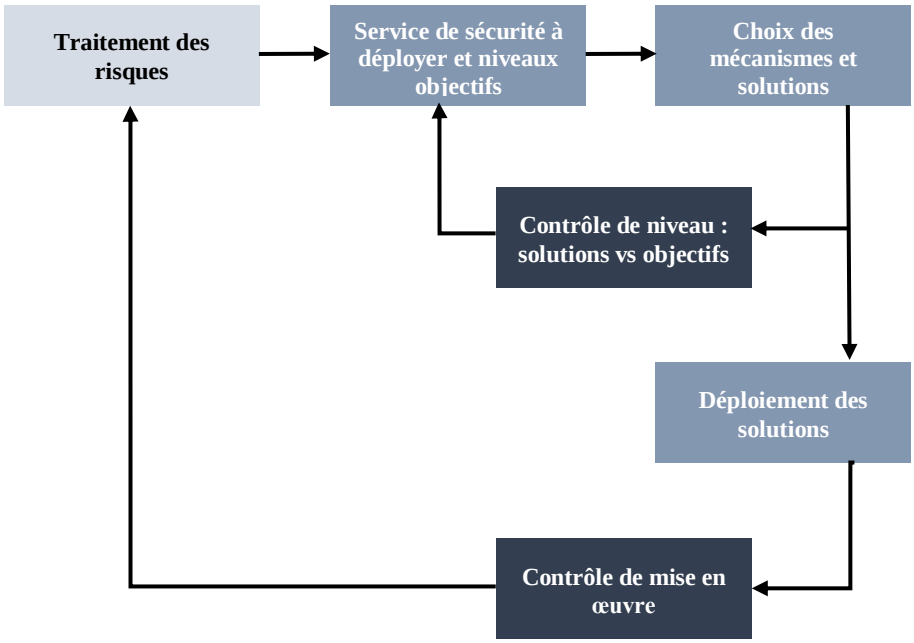
2. Choix des solutions : mécanismes techniques et organisationnels : Le choix des solutions relève des équipes spécialisées telles que la Direction des Systèmes d'Information (DSI), les responsables réseaux, les responsables de la sécurité physique, les RSSI, etc. Ces solutions sont regroupées dans un manuel de référence des services de sécurité, comprenant :

- L'objectif de chaque service.
- Les résultats attendus de la mise en œuvre du service.
- La description des mécanismes associés à chaque service, qu'ils soient techniques ou organisationnels.
- Les critères permettant d'évaluer la qualité de chaque service.

MEHARI propose un manuel de référence de services de sécurité.

Pour garantir leur efficacité, des contrôles doivent être effectués :

Figure 12: Processus contrôle



- Au premier niveau, pour vérifier que les mécanismes et solutions de sécurité planifiés correspondent aux niveaux de qualité de service retenus lors du traitement des risques.
- Au deuxième niveau, pour contrôler la mise en œuvre effective de ces solutions.

Ce chapitre met en avant l'importance cruciale de la gestion des risques, de la gouvernance informatique et de l'audit dans le domaine des systèmes d'information. La gestion des risques permet d'identifier, d'évaluer et d'atténuer les menaces potentielles pesant sur les systèmes informatiques, tandis que la gouvernance informatique établit les structures et les processus nécessaires pour une utilisation efficace et sécurisée des technologies de l'information. L'audit IT joue un rôle essentiel dans la vérification et l'assurance de la conformité des pratiques et des processus informatiques avec les normes et les objectifs organisationnels.

Dans le prochain chapitre, nous aborderons le cadre méthodologique et examinerons le contexte organisationnel dans lequel notre étude se déroule. Cette analyse approfondie nous permettra de mieux situer notre étude et d'expliquer comment nos résultats s'inscrivent dans cette organisation.

CHAPITRE II : CADRE MÉTHODOLOGIQUE ET CONTEXTE ORGANISATIONNEL

Dans ce chapitre, nous décrivons la méthodologie de notre étude et examinons le contexte organisationnel qui la définit, dans le but de mieux comprendre l'environnement dans lequel notre recherche se déroule.

1. Cadre Méthodologique

1.1 Approche épistémologique :

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

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

1.2 Approche méthodologique

Nous avons opté pour une approche méthodologique qualitative dans le but de répondre à nos objectifs de recherche. Car elle vise à développer une compréhension approfondie des pratiques de gestion des risques à appliquer lors d'une activité d'audit dans le cadre de la gouvernance des technologies de l'information (IT). En se concentrant sur les perceptions et les expériences des acteurs impliqués dans ces processus, notre objectif est d'explorer en profondeur ces domaines plutôt que de simplement confirmer ou infirmer des hypothèses prédéfinies. À travers des méthodes telles que les entretiens semi-structurés, l'observation participante et l'analyse documentaire, Nous viserons à saisir la diversité des points de vue des parties prenantes impliquées. En favorisant une immersion dans le terrain de recherche, nous aspirons à obtenir des données riches et nuancées qui nous permettront de construire une analyse approfondie et contextuellement informée.

1.3 Méthode de collecte de données

- **La recherche documentaire**

Dans le cadre de notre étude, nous avons mené une recherche documentaire approfondie en utilisant diverses sources d'informations telles que les données internes de l'entreprise, les sites web et les informations publiques. Cette étape, essentielle avant notre étude empirique, nous a permis de collecter des données informatives à partir des documents fournis par l'entreprise.

Selon Kenneth R. Bain dans "L'Art de la lecture"[1], la recherche documentaire est un processus dynamique et créatif qui consiste à explorer, découvrir et comprendre les connaissances existantes sur un sujet donné, tout en restant ouvert aux nouvelles idées et aux perspectives changeantes. En nous appuyant sur cette approche, nous avons analysé de manière critique les théories actuelles pertinentes à notre sujet, en nous basant sur une diversité de ressources telles que des livres, des thèses disponibles au sein de la bibliothèque de l'École Nationale Supérieure de Management (ENSM), ainsi que des articles académiques de recherche accessibles en ligne.

- **Sélection des interviewés**

Dans la sélection de nos interlocuteurs, nous avons opté pour une approche d'échantillonnage raisonné, inspirée de la méthode préconisée par Thiétart et ses collègues en 2014. Ce processus, également désigné comme "sampling par jugement", repose sur le discernement du chercheur dans le choix des participants. Il est considéré aussi efficace que les méthodes probabilistes, notamment pour des échantillons de petite taille.

Dans le cadre de cette étude, quatre entretiens ont été menés. Les trois premiers ont eu lieu avec les auditeurs participant à la mission, sélectionnés en fonction de leur expertise et de leur disponibilité. Le quatrième entretien a été réalisé avec la Direction des Systèmes d'Information (DSI) de l'organisation auditée, en raison de leur responsabilité cruciale dans la gestion et la sécurité des actifs informatiques.

Nos interviewés pour les entretiens directifs sont donc choisis en fonction de leur expérience et de leurs contributions aux missions de gestion des risques. Les entretiens ont été menés en personne ainsi que par téléphone avec l'accord préalable des interviewés, et des enregistrements ont été effectués dans le respect des consentements obtenus.

Tableau 4: liste des interviewés

Interviewé	profession	justification	Date et lieu	Durée

[1] L'Art de la lecture : La lecture documentaire dans un processus de recherche et de création, Kenneth R. Bain, 1984

Interviewé 01	Auditeur junior KPMG Algérie	Membre du groupe de la mission traitée	21-04-2014 l'entreprise	40min
Interviewé 02	Auditeur junior KPMG France ETE	Membre du groupe de la mission traitée	20-04-2014 l'entreprise	45min
Interviewé 03	Auditeur senior KPMG France ETE	Responsable de la mission traitée	18-04-2014 l'entreprise	45min
DSI	Directeur système d'information	Responsable des actifs audités	23-05-2025 (à distance)	1h

Le guide d'entretien

Notre premier guide d'entretien, destiné aux auditeurs est structuré de la manière suivante :

- **Thème 1 : Renseignements**

  Les questions sur le répondant visent à mieux comprendre les participants à l'entretien, leurs expériences, leur potentiel et différents aspects de leur carrière.

- **Thème 2 : Gestion des accès**

  Cette rubrique explore divers aspects de la gestion des accès, notamment l'authentification des utilisateurs, les politiques de mots de passe et la révocation des accès. Il aborde également la gestion des autorisations, la sécurité physique des accès.

- **Thème 3 : Gestion des incidents**

  La 3éme rubrique est composé de 5 questions et explore le processus de gestion des incidents dans les systèmes, y compris l'identification, la documentation et la priorisation des incidents.

- **Thème 4 : Gestion des changements**

  Cette partie couvre l'alignement des politiques, les processus de conception, d'intégration et de test des changements.

- **Thème 5 : Gestion des opérations informatiques**

  Dans la 5eme rubrique les questions portent sur la gestion opérationnelle des systèmes informatiques, incluant la révision des politiques de sauvegarde et de détection des intrusions.

- **Clôture :** Pour terminer, l'entretien se clôture par des remerciements et une dernière question ouverte pour encourager d'éventuelles remarques supplémentaires de la part de l'interviewé.

Le deuxième guide d'entretien orienté vers la direction des systèmes d'information (DSI) de l'organisation auditée, est organisé comme suit :

Nous aborderons trois thèmes cruciaux qui reflètent les applications auditées. Chacun de ces thèmes suivra une structure similaire, en explorant les mêmes sujets clés :

- l'utilité des applications auditées.
- Mesure de la criticité des applications auditées par couche.
- l'analyse des processus métier et de support que les applications auditées prennent en charge.
- l'évaluation de la criticité des processus des applications auditées.

En utilisant cette approche cohérente, nous pourrons obtenir une compréhension approfondie de l'impact et de l'importance de ces applications et processus pour les opérations bancaires.

- **Thème 1 :** SWIFT
- **Thème 2 :** Core Banking System
- **Thème 3 :** Service Desk et ITSM
- **Clôture :** l'interview prend fin avec une expression de gratitude.

- **Traitement des données**

Selon Miles & Huberman (1994), il est crucial de reconnaître que l'étape de traitement des données ne dispose pas d'une solution universelle, mais plutôt d'une gamme variée d'outils, de techniques et de méthodes qui peuvent être adaptés en fonction des besoins spécifiques de chaque projet. Ces approches offrent une méthodologie systématique pour organiser, analyser et interpréter les informations recueillies.

Après avoir recueilli les réponses des auditeurs, nous avons d'abord procédé à une analyse manuelle de ces données. Cette approche nous a permis d'identifier les risques potentiels mentionnés par les auditeurs et d'acquérir une compréhension approfondie de leur contexte spécifique ainsi que de leur gravité potentielle.

Ensuite, nous avons choisi d'adopter la méthode de traitement des risques "MEHARI". Cette méthode s'avère indispensable pour traiter et évaluer les risques de manière approfondie. Elle offre un cadre structuré permettant de recenser les risques, d'évaluer leur probabilité d'occurrence ainsi que leur impact potentiel, et de proposer des plans d'action pour les aborder de manière adéquate.

2. Contexte organisationnel

KPMG, une boîte internationale qui opère dans 156 pays avec plus de 156 000 professionnels, est arrivée en Algérie en 2002 et a réussi à se frayer un chemin sur ce marché, rivalisant même avec d'autres membres des "Big Four" comme Ernst & Young, Deloitte et Price Waterhouse Cooper.

Dans cette section, on va explorer en trois parties différentes la présentation de KPMG. La première partie va parler de l'entreprise à l'échelle mondiale. Ensuite, on va regarder sa position au niveau national. Enfin, on va détailler les différents services proposés par KPMG Algérie SPA ainsi qu'une analyse SWOT de cette dernière.

2.1 KPMG

2.1.1 Histoire et structure

L'histoire de cette organisation remonte à trois siècles. Tout a commencé en 1818 lorsque John Moxham a créé une entreprise à Bristol appelée "John Moxham & Co". En 1857, James Grace et James Grace Jr ont repris cette entreprise, la renommant "James Grace & Son". En 1861, Henry Grace les a rejoints, et l'entreprise est devenue "James & Henry Grace".
De son côté, William Barclay Peat a débuté sa carrière en rejoignant "Robert Fletcher & Co" à Londres en 1891, qui a ensuite été rebaptisée "William Barclay Peat & Co". En 1877, Thomson McLintock a fondé "Thomson McLintock & Co" à Glasgow. En 1897, James Marwick et Roger Mitchell ont créé "Marwick Mitchell & Co" à New York, et Ferdinand William LaFrentz a fondé "The American Audit Co" à New York en 1899.
À travers diverses fusions et acquisitions, des entités majeures telles que "Peat Marwick Mitchell & Company" ont été formées en 1925, puis "KPMG" en 1987 après la fusion de "KMG" et "Peat Marwick". En 1990, ces sociétés ont fusionné sous le nom de "KPMG Peat Marwick McLintock", avant d'être rebaptisées "KPMG" en 1991.
Au fil des décennies, KPMG a étendu ses activités, notamment en renforçant son secteur de conseil par l'acquisition de sociétés comme "Softline Consulting".

1. **Création et origine du nom :**

Fondé en 1987 par la fusion de Peat Marwick International (PMI) et Klynveld Main Goerdeler (KMG).

Le nom "KPMG" est formé des initiales des noms des principaux fondateurs des cabinets membres :

K : Klynveld (Piet Klynveld, fondateur de Klynveld Kraayenhof & Co. à Amsterdam en 1917)

P : Peat (William Barclay Peat, fondateur de William Barclay Peat & Co. à Londres en 1870)

M : Marwick (James Marwick, cofondateur de Marwick, Mitchell & Co. à New York en 1897)

G : Goerdeler (Dr. Reinhard Goerdeler, ancien président de Deutsche Treuhand-Gesellschaft et de KPMG, a joué un rôle crucial dans la fusion KMG)

2. **Domaines d'intervention :**

Audit financier

Fiscalité

Conseil

2.2 KPMG Algérie SPA :

2.2.1 Fondation et expansion :

KPMG Algérie SPA, membre du groupe KPMG, a été créé en 2002, devenant ainsi le premier cabinet international d'audit et de conseil à s'installer en Algérie. Depuis lors, conscient des changements vers la libéralisation dans le pays et des nouveaux besoins des entreprises, KPMG a continué à renforcer son expertise en comprenant les réalités historiques, culturelles, politiques et économiques locales, lui permettant ainsi de répondre efficacement aux exigences du marché.

Aujourd'hui, KPMG Algérie SPA est un leader sur le marché algérien en proposant une gamme complète de services d'audit et de conseil à une clientèle variée, nationale et internationale, dans tous les secteurs d'activité.

L'équipe de KPMG, composée de N personnes, dont Y associés, X managers et Z consultants, agit avec un engagement envers la durabilité, l'éthique, l'indépendance et la qualité, en conformité avec les normes et méthodes de KPMG International.

2.2.2 Services offerts :

KPMG Algérie SPA propose une gamme complète de services professionnels pour répondre aux besoins des entreprises algériennes dans divers secteurs d'activité.

Les trois principaux services offerts par KPMG Algérie SPA sont :

2.2.2.1 Audit et Conseil :

- **Audit financier :** Certification des états financiers selon les normes comptables en vigueur.
- **Audit interne et conseil en gestion :** Amélioration des processus et de la performance des entreprises.
- **Conseil en risques :** Évaluation et gestion des risques liés aux opérations, à la finance et à la technologie.
- **Transaction Advisory :** Accompagnement dans les opérations de fusion-acquisition et de cession.

2.2.2.2 Comptabilité et Services Administratifs :

- **Externalisation de la comptabilité :** Tenue des comptes et assistance à la production des déclarations fiscales.
- **Paie et RH :** Gestion de la paie et des ressources humaines.
- **Administration des sociétés :** Assistance dans la création et la gestion des sociétés.

2.2.2.3 **Fiscalité et Droit :**

- **Conseil fiscal :** Optimisation de la fiscalité des entreprises et assistance à la conformité.
- **Conseil juridique :** Assistance dans les domaines du droit des affaires, du droit du travail et du droit fiscal.

En plus de ces trois services principaux, KPMG Algérie SPA propose également des services spécialisés dans les domaines suivants :

- **Cybersécurité :** Évaluation des risques cybernétiques, mise en place de mesures de sécurité informatique et réponse aux incidents de sécurité.
- **Transformation digitale :** Accompagnement des entreprises dans leur transformation digitale, y compris l'adoption de nouvelles technologies, la refonte des processus métiers et la gestion du changement.
- **Consulting en développement durable :** Aide les entreprises à intégrer les principes du développement durable dans leur stratégie et leurs opérations, y compris la réduction de l'empreinte carbone, l'amélioration de la performance environnementale et sociale et la contribution aux objectifs de développement durable.

2.2.3 Clients :

KPMG est en mesure d'anticiper et de proposer des solutions adaptées aux besoins des principaux secteurs économiques, grâce à son large éventail de clients nationaux et internationaux opérant dans divers domaines tels que :

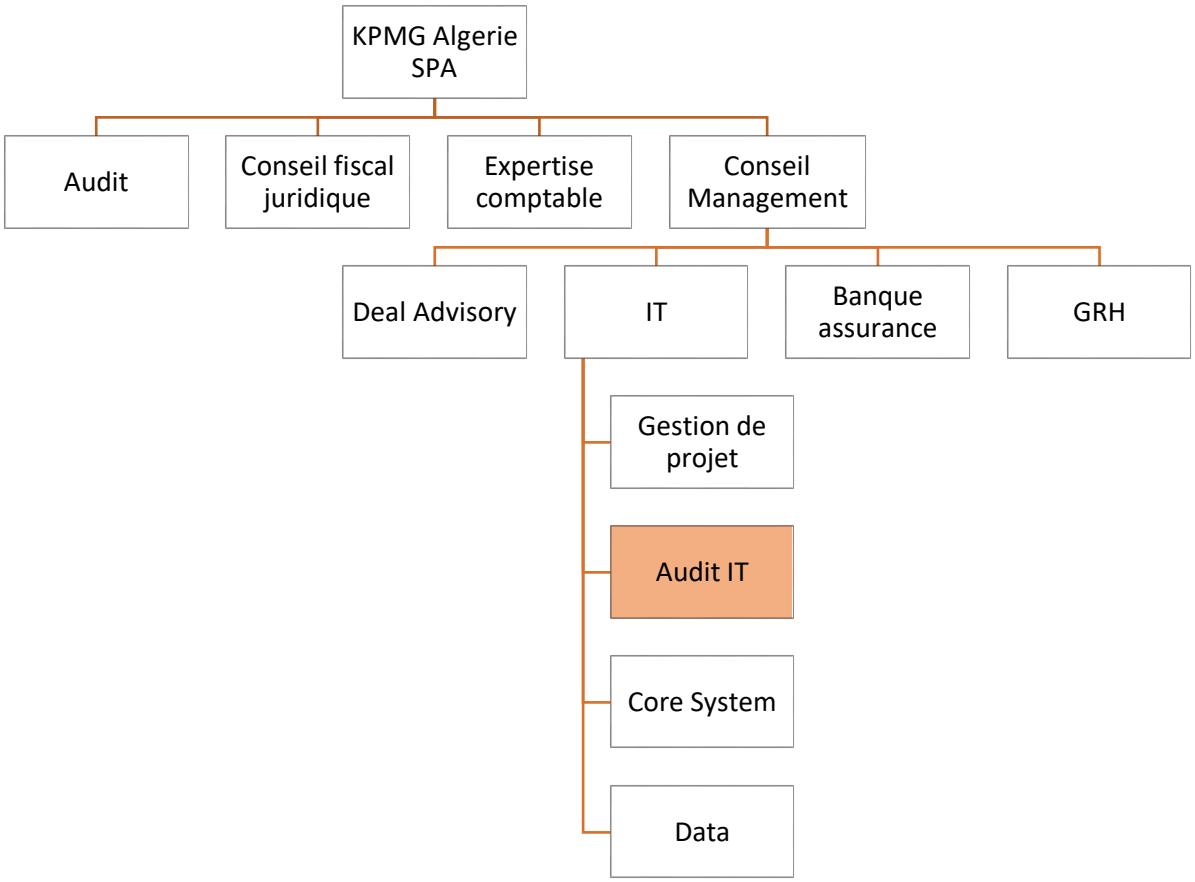
- Finance : banques, assurances
- Industrie : automobile, pharmacie, énergie, transport, construction, etc.
- Technologie : électronique, communication, informatique, etc.
- Consommation : agroalimentaire, etc.
- Loisirs : tourisme, hôtellerie, etc.
- Éducation et formation.

2.2.4 Positionnement :

L'un des principaux cabinets d'audit et de conseil en Algérie

2.2.5 Organigramme :

Figure 13: Organigramme KPMG Algérie SPA



L'organigramme de KPMG Algérie SPA est élaboré de manière à fournir une gamme étendue de services professionnels répondant aux besoins variés des clients. Ce modèle organisationnel met en lumière la diversité des départements et des spécialités au sein de l'entreprise, chacun contribuant de manière distincte à la mission globale de KPMG.

2.2.5.1 **Audit *:***

Ce département occupe une position cruciale dans l'évaluation de la fiabilité et de la conformité des comptes des clients de KPMG. Il s'engage à garantir que les informations financières sont complètes, sincères et régulières, assurant ainsi la confiance des parties prenantes et le bon déroulement des opérations sur les marchés financiers. Le processus d'audit est essentiel pour évaluer la santé financière d'une entreprise et identifier tout écart potentiel qui pourrait nécessiter une correction.

2.2.5.2 **Conseil fiscal et juridique *:***

Ce département offre des conseils spécialisés sur les questions fiscales et juridiques, agissant comme un guide stratégique pour les clients dans tous les aspects de leurs activités. En plus de l'audit et de la révision fiscale, il fournit une assistance à la mise en conformité et une due diligence pour assurer la conformité réglementaire et minimiser les risques juridiques.

2.2.5.3 Expertise comptable :

Ce service propose une gamme étendue de services comptables, incluant la tenue de livres, la gestion de la paie, les déclarations fiscales et la gestion de trésorerie. Grâce à cette expertise, les clients peuvent externaliser efficacement leurs besoins comptables et se concentrer sur leur cœur de métier, tout en bénéficiant d'un suivi financier précis et fiable.

2.2.5.4 Conseil Management *:*

Ce département accompagne les entreprises dans la planification et la mise en œuvre de projets de transformation et d'amélioration de la performance. En travaillant sur divers aspects, tels que les opérations, la finance et les systèmes d'information, il vise à optimiser les processus internes et à renforcer la compétitivité des clients sur le marché.

2.2.5.4.1 Deal Advisory :

Ce département apporte une expertise spécialisée aux entreprises dans le cadre de leurs transactions, visant à maximiser la valeur ajoutée lors de ces opérations. Grâce à des équipes dédiées, il aide les clients à naviguer à travers les défis liés aux fusions, acquisitions et cessions d'entreprise.

2.2.5.4.2 IT :

Ce département est responsable de la gestion des systèmes informatiques et se divise en plusieurs groupes spécialisés :

- **Gestion de projet** : Ce groupe est responsable de la planification, de la coordination et de la supervision des projets au sein de l'entreprise, garantissant ainsi leur bonne exécution dans les délais et le budget impartis. Il assure également la coordination efficace des ressources et des équipes impliquées dans les projets de l'entreprise.
- **Core System (Système central) :** Ce groupe est chargé de la gestion et de la maintenance des systèmes informatiques centraux de l'entreprise, qui sont essentiels pour soutenir ses opérations quotidiennes. Il veille à ce que ces systèmes soient fiables, sécurisés et conformes aux normes pour garantir la continuité des activités de l'entreprise.
- **Audit IT :** Ce groupe est dédié à l'évaluation et à l'analyse des systèmes informatiques à travers des missions d'audit IT. Son objectif principal est d'assurer la sécurité, l'intégrité

et l'efficacité des systèmes, en vérifiant les contrôles de sécurité, en identifiant les risques potentiels et en recommandant des mesures correctives pour améliorer la performance et réduire les risques.

- **Data (Données) :** Ce groupe est responsable de la gestion et de l'analyse des données au sein de l'entreprise. Il s'assure que les données sont collectées, stockées, traitées et utilisées de manière sécurisée et conforme aux réglementations en vigueur. Il fournit également des analyses de données pertinentes pour aider l'entreprise à prendre des décisions stratégiques basées sur des données fiables et précises.

2.2.5.5 Banque et assurance *:*

Ce département fournit des services spécialisés aux clients du secteur financier, offrant une expertise approfondie dans les défis spécifiques de ce domaine.

2.2.5.6 GRH *:*

Responsable de la gestion des ressources humaines de l'entreprise, ce département veille à attirer, à développer et à retenir les talents, assurant ainsi la force de travail nécessaire pour atteindre les objectifs stratégiques de l'entreprise.

Cette organisation rigoureuse et multidisciplinaire permet à KPMG Algérie SPA de répondre de manière efficace et complète aux besoins complexes et évolutifs de ses clients, contribuant ainsi à leur succès et à leur croissance à long terme. Chaque département, avec ses spécialités uniques, constitue un maillon essentiel dans la chaîne de valeur ajoutée que l'entreprise offre à ses clients.

2.2.6 Hiérarchie de l'équipe d'audit

Pour chaque mission d'audit, l'équipe qui traite le dossier est composée de membres suivants :

• L'associé **:** son rôle est la revue des rapports et des dossiers d'audit, l'approbation de la stratégie d'audit et la signature des comptes ;

• les managers et superviseur **:** constitue la charpente même de l'édifice. Il s'occupe, en effet, de mettre en place la stratégie d'audit, des discussions des rapports avec le client, et de la revue des dossiers et des travaux de l'équipe ;

• Senior **:** il s'occupe de la supervision de l'équipe sur le terrain, dirige les assistants du groupe dans l'accomplissement des missions. Il est aussi chargé de la revue des travaux du junior ;

• le junior : ce sont des exécutants des programmes, ils effectuent toutes les tâches consignées sous la supervision du senior. Cependant, les tâches incombées au sénior sont importantes par rapport à celles du junior.

Ce chapitre a permis d'établir les fondements méthodologiques de notre étude ainsi que de définir le contexte organisationnel dans lequel elle se situe. Nous avons détaillé notre approche méthodologique, en mettant en lumière notre choix épistémologique et notre méthode de collecte de données, ce qui établit une base solide pour la conduite de notre recherche. De plus, notre exploration du contexte organisationnel, en se concentrant sur KPMG et sa filiale en Algérie, KPMG Algérie SPA, nous a permis de mieux comprendre les paramètres externes et internes qui influenceront notre travail. Cette analyse approfondie nous fournira une perspective précieuse pour interpréter nos résultats et élaborer des recommandations pertinentes.
En somme, ce chapitre prépare le terrain pour la suite de notre étude qui sera une étude de cas pratique portant sur un client de KPMG, en nous fournissant les outils nécessaires pour mener à bien notre recherche dans un cadre méthodologique approprié et un contexte organisationnel bien défini.

CHAPITRE III : Résultats et discussions

Introduction

Dans ce chapitre, nous passerons à la concrétisation de notre mémoire en mettant en avant les analyses qualitatives de notre étude. Nous explorerons les implications pratiques de nos recherches et examinerons de près les données recueillies. Enfin, nous tirerons des conclusions éclairées sur les résultats obtenus, offrant ainsi un aperçu complet de notre travail.

1. Étude de l'existant :

Chez KPMG, l'approche adoptée repose sur une méthodologie complète et éprouvée, en conformité avec les normes internationales telles que l'International Standard on Auditing (ISA 315 (Revised 2019). Cette approche vise à identifier et répondre aux risques informatiques qui peuvent avoir un impact sur les états financiers, contribuant ainsi à la protection des actifs et à la fiabilité des informations financières de ses clients.

l'auditeur de chez KPMG utilise ISA 315 (Revised 2019) pour fournir une assurance raisonnable sur la fiabilité des systèmes d'information de l'entreprise et sur la validité des données financières qui en découlent. En évaluant les contrôles internes, en identifiant les risques potentiels et en testant l'efficacité des contrôles existants, l'auditeur peut formuler une opinion sur l'intégrité des processus informatiques de l'entreprise et la qualité de l'information financière qui en découle. Cette assurance est essentielle pour les parties prenantes internes et externes de l'entreprise, telles que les actionnaires, les dirigeants et les régulateurs, afin de prendre des décisions éclairées.

Bien que l'approche de KPMG basée sur l'ISA 315 fournit une base solide pour identifier et évaluer les risques liés aux systèmes d'information, MEHARI offre une perspective supplémentaire en se concentrant spécifiquement sur l'analyse et le traitement des risques liés à la sécurité de l'information. En intégrant MEHARI à notre démarche d'audit, nous pouvons bénéficier d'une analyse plus approfondie des risques de sécurité et des mesures de contrôle associées, ce qui renforce notre capacité à identifier les vulnérabilités potentielles et à recommander des actions correctives appropriées.

Tableau 5: Tableau comparatif entre ISA 315 et MEHARI

	ISA 315 (Révisée 2019)	MEHARI
Objectif principal	Évaluer l'efficacité des contrôles internes et des processus informatiques	Évaluer et gérer les risques de sécurité des SI
Portée	Plus large, couvrant l'ensemble des processus informatiques, y compris la gouvernance, la gestion des risques, etc.	Plus ciblée sur les risques de sécurité de l'information
Méthodologie	Approche structurée basée sur les risques	Méthodologie structurée en six étapes : Mesure, Examen, Harmonisation, Analyse, Réponse et Information
Utilisation des résultats	Formulation de recommandations pour améliorer les contrôles internes et les processus informatiques	Guide la mise en œuvre de mesures de sécurité spécifiques et priorise les investissements en sécurité informatique
Avantages	Fournit un cadre solide pour identifier, évaluer et répondre aux risques informatiques	Permet une analyse plus approfondie des risques de sécurité de l'information
Limites	Peut ne pas identifier toutes les vulnérabilités potentielles, en particulier en matière de sécurité de l'information	Ne couvre pas tous les aspects des processus informatiques
Intégration	Peut être utilisée seule ou en combinaison avec MEHARI pour une évaluation plus complète des risques	Complète l'ISA 315 en offrant une perspective supplémentaire sur la sécurité de l'information

Avantages pour KPMG et ses clients

L'intégration de MEHARI dans les processus d'audit permettra à KPMG d'offrir à ses clients une évaluation plus exhaustive des risques liés à la sécurité de l'information, ce qui renforcera la qualité et la pertinence des recommandations en matière de gouvernance IT. De plus, en

utilisant une méthodologie reconnue comme MEHARI, KPMG démontre son engagement envers les meilleures pratiques internationales en matière de gestion des risques.

En combinant l'approche robuste de l'ISA 315 de KPMG avec la méthodologie structurée de MEHARI, nous sommes bien positionnés pour fournir des services d'audit de haute qualité qui répondent aux besoins complexes de leurs clients en matière de gouvernance IT et de sécurité de l'information.

2. Résultats :

Pour mettre en œuvre la méthodologie Mehari, nous avons pris comme référence un client de KPMG du secteur bancaire. En collaborant étroitement avec les auditeurs impliqués dans cette mission ainsi que la DSI de ce client, nous avons pu adapter les principes et les processus de Mehari à leurs besoins spécifiques et aux exigences particulières de leurs industrie.

2.1 Appréciation des risques

2.1.1 Identification des risques

La norme ISA 315 (Révisée en 2019) propose une liste de risques et de points de contrôle, sur la base desquels les auditeurs de KPMG interrogés ont orienté leurs analyses lors de la mission d'audit IT.

Les contrôles IT se font sur quatre couches :

Tableau 6: Nature des couches contrôlées

Couche	Nature du contrôle
Applications	Les CGI au niveau des applications informatiques varient en fonction de leur complexité et de leurs fonctionnalités. Des applications hautement intégrées avec des options de sécurité sophistiquées nécessitent plus de contrôles que des applications internes simples. Les contrôles peuvent inclure des vérifications d'authentification et d'autorisation spécifiques à chaque application.
Base de données	Les CGI à ce niveau visent à prévenir les mises à jour non autorisées des données financières. Cela inclut la protection contre l'accès direct non autorisé ou l'exécution de scripts malveillants. Des contrôles peuvent

	inclure des restrictions d'accès basées sur les rôles et des audits réguliers des activités de la base de données.
Système d'exploitation	Les CGI pour les systèmes d'exploitation se concentrent sur les droits d'administrateur et d'autres privilèges élevés. Les risques incluent l'usurpation d'identité, l'ajout d'utilisateurs non autorisés, et l'exécution de logiciels malveillants. Les contrôles peuvent inclure la gestion stricte des comptes administratifs et la surveillance des modifications du système.
Réseau	Les CGI au niveau du réseau traitent de la segmentation du réseau, de l'accès à distance, et de l'authentification. Ces contrôles sont importants pour les applications web et les interactions avec des tiers. Les mesures peuvent inclure des pares-feux, des réseaux privés virtuels (VPN), et la surveillance des intrusions.

La liste des contrôles est structurée comme suite :

Tableau 7: Points de contrôle

Catégorie	Aspect	Risques	Contrôles	Applicabilité
Gestion des accès	**Authentification**	Utilisation d'identifiants partagés	Vérification que chaque utilisateur utilise son propre identifiant	Toutes les tailles d'applications
	Autorisation	Accès non nécessaires	Accès limité aux informations nécessaires pour les tâches	Toutes les tailles d'applications
	Attribution	Attributions inappropriées des droits	Gestion rigoureuse de l'attribution initiale des droits d'accès	Toutes les tailles d'applications
	Révocation	Accès après cessation d'emploi	Révocation rapide des droits d'accès	Toutes les tailles d'applications
	Accès privilégié	Abus de privilèges élevés	Gestion stricte des droits des administrateurs et des utilisateurs avec des privilèges élevés	Toutes les tailles d'applications
	Examen des accès	Droits d'accès inappropriés	Évaluation périodique des accès	Toutes les tailles d'applications

	Paramètres de sécurité	Accès non autorisé	Configurations de sécurité restrictives	Toutes les tailles d'applications
	Accès physique	Contournement des contrôles	Contrôle de l'accès physique aux centres de données	Toutes les tailles d'applications
Gestion des changements	**Processus de gestion**	Changements non supervisés	Supervision de la conception, la programmation, les tests et l'intégration des changements	Essentiel pour logiciels non commerciaux et grandes applications
	Séparation des tâches	Conflits d'intérêt	Séparation entre ceux qui effectuent les changements et ceux qui les intègrent en production	Essentiel pour logiciels non commerciaux et grandes applications
	Élaboration et mise en œuvre des systèmes	Intégration inadéquate des mises à niveau	Contrôle rigoureux des nouvelles applications et des mises à niveau	Essentiel pour logiciels non commerciaux et grandes applications
	Conversion des données	Erreurs lors des conversions	Gestion rigoureuse de la conversion des données	Essentiel pour logiciels non commerciaux et grandes applications
Gestion des opérations informatiques	**Planification des travaux**	Impact négatif sur les données financières	Gestion de l'accès et du lancement des programmes	Requise pour toutes les tailles de systèmes
	Suivi des travaux	Dysfonctionnements non détectés	Surveillance continue des programmes	Requise pour toutes les tailles de systèmes
	Sauvegarde et récupération	Perte de données	Sauvegardes régulières et récupération rapide des données	Requise pour toutes les tailles de systèmes
	Détection des intrusions	Vulnérabilités et intrusions	Surveillance et traitement rapide des vulnérabilités et des intrusions	

À partir des résultats de nos entretiens avec les auditeurs et la DSI de la banque auditée, nous avons listé et évalué la criticité des actifs audités pour pouvoir identifier et élaborer une base de connaissance des risques liés à ces actifs, en suivant les étapes du processus d'identification des risques MEHARI :

Liste des actifs audités :

1. **SWIFT (Society for Worldwide Interbank Financial Telecommunication)**:
   - **Description** : SWIFT est un réseau international de messagerie financière sécurisé utilisé par les banques et les institutions financières pour échanger des informations financières de manière sécurisée. SWIFT facilite les transactions financières internationales, telles que les virements bancaires, les paiements et les confirmations de transactions.
2. **Core Banking System Application** :
   - **Description** : C'est un logiciel utilisé par les banques pour gérer leurs opérations bancaires courantes, telles que les dépôts, les retraits, les prêts, la gestion des comptes clients, et d'autres services financiers. Cet outil permet aux banques de centraliser et d'automatiser les processus bancaires essentiels, offrant une vue unifiée des transactions et des comptes clients.
3. **ITSM (IT Service Management) Application** :
   - **Description** : C'est un logiciel conçu pour soutenir et automatiser les processus de gestion des services IT, tels que la gestion des incidents, la gestion des changements, la gestion des configurations et la gestion des niveaux de service. Cela aide les équipes IT à fournir des services de haute qualité en suivant les meilleures pratiques ITIL (Information Technology Infrastructure Library) pour une gestion efficace des services IT.

4. **Service Desk Application** :
   - **Description** : C'est un outil utilisé pour gérer les demandes de support informatique et les incidents signalés par les utilisateurs. Elle permet de suivre, de prioriser et de résoudre les problèmes techniques de manière efficace.
   - **Utilisation** : Utilisée par les équipes de support informatique pour recevoir, suivre et gérer les tickets de support, offrant des solutions rapides aux problèmes des utilisateurs finaux.
     - Le Service Desk Application est souvent intégré à un cadre ITSM.

1 : Non significatif

Les dommages encourus n'ont pratiquement pas d'impact sur les résultats de l'entreprise ni sur son image.

2 : Important

Les dommages encourus ont un impact significatif au niveau des résultats de l'entreprise et de son image, mais restent largement supportables.

3 : Très grave

Les dommages encourus sont graves, et vont causer des pertes considérables

4 : Vital

A ce niveau les dommages encourus sont extrêmement graves et mettent en danger l'existence de l'entreprise (la disparition de l'une de ses activités majeures)

Disponibilité (D) : Un score de 4 indique un risque élevé de non-disponibilité.

- Par exemple, si les serveurs SWIFT subissent des pannes fréquentes, cela peut entraîner des interruptions dans les transactions financières.

Intégrité (I) : Un score de 4 indique un risque élevé pour l'intégrité des données.

- Par exemple, si les données SWIFT sont sujettes à des modifications non autorisées, cela peut compromettre la validité des transactions.

Confidentialité (C) : Un score de 4 indique un risque élevé pour la confidentialité des données.

- Par exemple, si les informations sensibles échangées via SWIFT sont compromises, cela peut entraîner des fuites de données confidentielles.

Tableau 8 : degré de criticités des actifs par couche

	SWIFT			**Core Banking System Application**			**Service Desk Application ITSM Application**		
	D	I	C	D	I	C	D	I	C
APPLICATIVE	4	4	4	4	4	4	4	3	3
BDD	4	4	4	4	4	4	4	2	2
OS	4	4	4	4	4	4	4	1	1

Tableau 9: degré de criticité des actifs par processus

	SWIFT			Core Banking System Application			Service Desk Application ITSM Application		
	D	I	C	D	I	C	D	I	C
Processus métier									
Rapport financier				4	4	4	3	2	3
Gestion des compte clients				4	4	4			
Prêt et crédit				4	4	4			
Les services de paiement				4	4	4			
Provision pour pertes sur créances				4	4	4			
Dépôts et retrait				4	4	4			
Trésorerie				4	4	4			
Gestion des paiements	4	4	4						
les virements	4	4	4						
échanges de devises	4	4	4						
Messagerie financière	4	4	4						
Surveillance des transactions	4	4	4				3	3	4
Gestion des tickets							4	4	4
Conformité réglementaire	4	4	4				3	3	4
Processus support									
Gestion des clés de sécurité	4	4	4	4	4	4	4	4	4
Développement technologique	2	3	3	3	3	3	3	2	2
Gestion des membres	4	3	3	3	3	4	4	4	4
Gestion de la Continuité des IT	4	4	4	4	4	4	4	4	4
Gestion des Changements	4	4	4	3	3	3	4	4	4
Gestion des Problèmes	4	4	4	3	3	4	4	4	4
Gestion des Incidents	4	4	4	4	4	4	4	4	4
Gestion de la configuration	4	4	4	2	2	4	3	3	3
Gestion des demandes de service	4	4	4	4	4	3	4	4	4

La gestion efficace des systèmes ITSM, Core Banking et SWIFT est cruciale pour garantir la disponibilité, la continuité et l'intégrité des services financiers et informatiques essentiels. Ces systèmes sont au cœur des opérations bancaires quotidiennes, de la gestion des services informatiques et des transactions financières internationales, et leur bon fonctionnement est indispensable à la stabilité et à la sécurité de ces activités vitales. Par conséquent, il est impératif d'identifier les risques associés à ces systèmes.

Tous les risques et défaillances identifiés font partie de ces domaines :

- Gestion des accès
- Gestion des changements
- Gestion des opérations informatiques
- Gestion de continuité
- Gestion de la conformité

Tableau 10: base de connaissances

Défaillance	Processus	Risque	Observation	Conséquence
1. **Absence des résultats des tests de restauration des sauvegardes pour les applications critiques**	Gestion des opérations informatiques	• Échec de la restauration des données en cas de besoin (incident).	Les sauvegardes sont restaurées à la demande, mais la politique exige une restauration mensuelle pour Core Banking System Application, SWIFT APP, ITSM. Les résultats des tests ne sont pas documentés.	• incapacité d'évaluer la fiabilité des processus de sauvegarde qui peut entraîner une perte de données en cas de panne ou de catastrophe du système voir interruption des opérations et donc l'arrêt d'activité.
2. **Processus de désactivation des accès utilisateurs retardé**	Gestion des accès	• Accès non autorisé aux applications. • Accès direct aux données	Retard dans la désactivation de l'accès utilisateur pour les utilisateurs mentionnés (annexe B01) dans l'application Core Banking System Application, SWIFT APP, ITSM	• Transactions non autorisées. • Vol. • Corruption ou destruction de données. • Fraude.

3. Non-conformité des paramètres de mot de passe aux normes de l'industrie	Gestion des opérations informatiques	• Accès non autorisé • Accès direct aux données	Le système actuel ne respecte pas pleinement les normes de l'industrie en matière de sécurité des mots de passe et de verrouillage de compte. Les paramètres actuels sont moins stricts, comme détaillé dans l'annexe B02. Core Banking System Application, SWIFT APP	• Système vulnérable aux attaques. • Perte de la confidentialité et la crédibilité des données au sein des systèmes d'application.
4. Lacunes dans les examens d'accès des utilisateurs	Gestion des accès	• Accès non autorisé • Accès direct aux données. • Privilèges d'accès	Absence d'une évaluation fréquente(contrôle) des profils d'accès des utilisateurs, les utilisateurs du système peuvent disposer d'autorisations d'accès qui dépassent leurs exigences fonctionnelles. Core Banking System Application, SWIFT APP, ITSM	• Un accès illégal au système. • Possibilité de publier, exécuter ou autoriser des transactions indésirables impactant potentiellement les états financiers. • Utilisation inappropriée des données.
5. Utilisation d'un compte utilisateur générique pour accéder à la salle des serveurs	Gestion des accès	• Accès non autorisé (Intrusion)	Lors de l'examen des logs d'accès, l'utilisation d'une carte d'accès avec le nom d'utilisateur générique "Admin_Generic_Name" a été observée.	• Accès plus facile et non autorisé à la salle des serveurs • Sécurité compromise. • Absence de responsabilité individuelle. • l'exploitation ou l'usurpation d'identité. • Effectuation des tâches et des fonctions privilégiées au sein des systèmes informatique.
6. Politiques et procédures informatiques non mises à jour	Gestion de la conformité	• Mise en œuvre incohérente des meilleures	• L'audit a révélé que certaines politiques et procédures informatiques de la BANQUE_XYZ ne sont pas	• Non-conformité réglementaire • Difficulté à mettre en œuvre des meilleures pratiques informatiques,

		pratiques informatiques • Mauvaise prise de décision	à jour ou complètes. Cela inclut : • Des politiques qui n'ont pas été révisées pour l'année 20XX. • Absence de définition de la fréquence d'examen des accès des utilisateurs dans les politiques. • Incohérence entre les SLA définis dans l'outil de billetterie XYZ_Ticketting_Tool et les SLA définis dans la politique.	compromettant la conformité et la gestion efficace des accès utilisateurs. • Système vulnérable • Prise de décision inefficace en cas d'incident de sécurité
7. Absence de tests de reprise après sinistre pour certaines applications critiques.	Gestion de continuité	• Incapacité à restaurer les systèmes et les données en cas de sinistre.	Aucun test de reprise après sinistre n'a été effectué pour l'applications CORE BAKING SYSTEM	• Impossible de garantir l'efficacité du DRP (Disaster Recovery Plan) et donc la non disponibilité, la non continuité des opérations.
8. Lacunes dans le processus de gestion du changement	Gestion des changements	• Mise en œuvre de changements non approprié, non réussi, non autorisées ou mal testées	• Les modifications sont enregistrées via trois canaux distincts (Un logiciel de gestion de projet, outil de ticketing et les e-mails.) • Malgré la mise en production (Go-Live), une demande de modification de ticket est restée ouverte sans être clôturée. • Les tests d'acceptation utilisateur (UAT) ont été effectués après le déploiement effectif (Go-Live) des modifications.	• Impact négativement la stabilité et la fiabilité du système • Conversion des données incomplètes, redondantes, obsolètes ou inexactes dans le nouveau système. • Dispersion des informations à travers plusieurs systèmes et donc perte d'information • Indisponibilité des systèmes

			l'annexe B03.	
9. Défaillances identifiées dans le processus de gestion des incidents	Gestion des opérations informatiques	• Un traitement incomplet, inexact, retardé ou non autorisé des données. • Priorisation mal des incidents	Priorité des incidents mal sélectionnée et certains incidents n'ont pas été résolus dans le cadre du SLA défini par la politique. Annexe B04	• Sanctions contractuelles et légales en raison de non-conformité au SLA. • Violations des engagements contractuels, • une diminution de la satisfaction des utilisateurs, • gaspille du temps et des ressources ce qui impact négatif sur les performances et la fiabilité du service.
10. Déficiences dans la Surveillance des Tâches	Gestion des opérations informatiques	• Non-détection des erreurs ou échecs des tâches critiques. • dépendance excessive aux utilisateurs métiers	les tâches du système sont configurées selon un calendrier et une fréquence définie. Cependant, aucune alerte n'est configurée pour être envoyée en cas d'erreurs ou de tâches programmées non réussies. Le groupe/l'équipe de support informatique dépend des utilisateurs métiers pour les notifier.	• La corruption des données • Des pannes du système ou des perturbations des processus métier. • Interruption des services.

2.1.2 Estimation et évaluation des risques :

Tableau 11: évaluation des risques

	PI	II	G	Facteurs de Réduction de la Potentialité	PR	Facteurs de Réduction de l'Impact	IR	G	Niveau de gravité
1. Absence des résultats des tests de restauration des sauvegardes pour les	3	4	4	- Existence de procédures de sauvegarde régulières	2	- Tests réguliers	3	3	Inadmissible

applications critiques									
2. Accès non autorisé aux applications	3	4	4	- Coordination et la communication proactive avec les parties prenantes (RH,RSSI, …)	2	- Révocation immédiate des accès non autorisés le plus tôt possible.	3	3	Inadmissible
3. Non-conformité des paramètres de mot de passe aux normes de l'industrie	4	4	4	- Mise à jour des configurations de mot de passe	3	- Aucun facteur détecté	4	4	Intolérable
4. Lacunes dans les examens d'accès des utilisateurs	3	4	4	- Planification de mise en place d'examens réguliers.	3	Aucun facteur détecté	4	4	Intolérable
5. Utilisation d'un compte utilisateur générique pour accéder à la salle des serveurs	4	4	4	- Élimination des comptes génériques - Attribution de comptes individuels	3	- Suivi des accès physiques - Contrôles d'accès renforcés	3	3	Inadmissible
6. Politiques et procédures informatiques non mises à jour	4	4	4	- Mise à jour et révision régulière des politiques - Alignement des SLA avec les politiques	3	Aucun facteur détecté	4	4	Intolérable
7. Absence de tests de reprise après sinistre pour certaines applications critiques.	4	4	4	- Planification et exécution régulière des tests DRP	3	Aucun facteur détecté	4	4	Intolérable
8. Lacunes dans le processus de gestion du changement	3	3	3	- Planification de formalisation du processus de gestion des changements - Documentation systématique	2	Aucun facteur détecté	3	3	Inadmissible

9. Défaillances identifiées dans le processus de gestion des incidents	3	3	3	- Mise en place de priorités dans le système de ticketing - Respect des SLA définis	2	Aucun facteur détecté	3	3	Inadmissible
10. Déficiences dans la Surveillance des Tâches	3	3	3	Aucun facteur détecté	3	Aucun facteur détecté	3	3	Inadmissible

*Potentialité intrinsèque (PI), Impact Intrinsèque (II), Gravité (G), Potentialité résiduelle (PR), Impact résiduel (IR)

2.2 Traitement des risques

Tableau 12:traitement des risques

	Accepter	Réduire	Transférer	Eviter
1. Absence des résultats des tests de restauration des sauvegardes pour les applications critiques		X		
2. Accès non autorisé aux applications		X		
3. Non-conformité des paramètres de mot de passe aux normes de l'industrie				X
4. Lacunes dans les examens d'accès des utilisateurs				X
5. Utilisation d'un compte utilisateur générique pour accéder à la salle des serveurs		X		
6. Politiques et procédures informatiques non mises à jour				X
7. Absence de tests de reprise après sinistre pour certaines applications critiques.				X
8. Lacunes dans le processus de gestion du changement		X		
9. Défaillances identifiées dans le processus de gestion des incidents		X		
10. Déficiences dans la Surveillance des Tâches		X		

2.3 Gestion des risques

2.3.1 Plan d'action

1. Défauts identifiés lors des tests de restauration des sauvegardes

Les défauts identifiés lors des tests de restauration des sauvegardes soulignent l'importance de vérifier régulièrement ces sauvegardes. Il est recommandé de tester les sauvegardes pour la restauration à intervalles fréquents, conformément à la politique établie. Les résultats de ces tests doivent être documentés de manière systématique. De plus, il est crucial de mettre en place un processus pour corriger les erreurs de restauration identifiées lors de ces tests.

Responsabilités	DSI	• Élaborer et mettre en œuvre un plan de test de restauration des sauvegardes. • Effectuer les tests de restauration des sauvegardes. • Documenter les résultats des tests de restauration. • Corriger les erreurs de restauration identifiées lors des tests.
	Utilisateurs	Coopérer aux tests de restauration des sauvegardes.
Calendrier	Immédiat	• Définir les exigences du plan de test de restauration des sauvegardes. • Identifier les ressources nécessaires.
	30 Jours	• Élaborer le plan de test de restauration des sauvegardes. • Dispenser une formation aux employés sur le nouveau plan.
	60 Jours	Commencer à effectuer les tests de restauration des sauvegardes.
	90 Jours	Effectuer un audit de suivi pour vérifier la mise en œuvre du nouveau plan et identifier tout domaine d'amélioration.
Annexes	• Rapport d'audit initial	

	• Plan de test de restauration des sauvegardes • Formulaire de résultats de test de restauration des sauvegardes • Programme de formation sur la restauration des sauvegardes

2. **Processus de désactivation des accès utilisateurs retardé**

Le processus de désactivation des accès utilisateurs est souvent retardé, ce qui pose des risques de sécurité. Il est recommandé de mettre en place un processus formel garantissant que l'accès des utilisateurs est révoqué au plus tard le dernier jour ouvrable de leur emploi. Ce processus doit être documenté et inclure les responsabilités de toutes les parties prenantes. Il est également essentiel de former les employés au nouveau processus de désactivation et de mettre en place des contrôles pour surveiller et assurer le respect de ce processus.

Responsabilités	DSI	Élaborer et mettre en œuvre le processus de désactivation des accès utilisateurs. Former les employés au nouveau processus. Surveiller le processus de désactivation et s'assurer qu'il est respecté.
	Ressources humaines	Communiquer les dates de départ des employés à la DSI en temps opportun.
	Managers	Approuver les demandes de désactivation des accès utilisateurs.
	Utilisateurs	• Coopérer aux tests de restauration des sauvegardes.
Calendrier :	Immédiat	Définir les exigences du processus de désactivation des accès utilisateurs. Identifier les ressources nécessaires.
	30 Jours	• Élaborer le processus de désactivation des accès utilisateurs. • Dispenser une formation aux employés sur le nouveau processus.
	60 Jours	• Mettre en œuvre le nouveau processus de désactivation des accès utilisateurs.
	90 Jours	• Effectuer un audit de suivi pour vérifier la mise en œuvre du nouveau processus et identifier tout domaine d'amélioration.

Annexes	Rapport d'audit initial Procédure de désactivation des accès utilisateurs Formulaire de demande de désactivation des accès utilisateurs Programme de formation sur la désactivation des accès utilisateurs

3. **Non-conformité des paramètres de mot de passe aux normes de l'industrie**

Les paramètres de mot de passe actuels ne sont pas conformes aux normes de l'industrie. Il est recommandé de suivre ces recommandations :

Configurations des mots de passe

Longueur minimale du mot de passe : 8 caractères (ANASSI : 12 caractères)

Historique des mots de passe : 24

Âge minimum du mot de passe : 1 jour

Âge maximum du mot de passe : 45 jours

Exigences de complexité du mot de passe : Activées

Des caractères spéciaux, comme des signes de ponctuation, des chiffres, des majuscules et des minuscules.

Configurations du verrouillage de compte

Seuil de verrouillage du compte : 3 tentatives de connexion invalides

Durée de verrouillage du compte : 15 minutes ou 0 minutes (verrouiller l'utilisateur indéfiniment)

Réinitialisation du compteur de verrouillage du compte : 30 minutes

Responsabilités	DSI	• Mettre à jour la politique de mots de passe et la documenter. • Mettre en œuvre les nouveaux paramètres de configuration des mots de passe. • Former les employés sur la nouvelle politique de mots de passe.
	Utilisateurs	• Respecter la nouvelle politique de mots de passe.
Calendrier	Immédiat	• Mettre à jour la politique de mots de passe. • Identifier les ressources nécessaires pour la mise en œuvre
	30 Jours	• Dispenser une formation aux employés sur la nouvelle politique de mots de passe.
	60 Jours	• Mettre en œuvre les nouveaux paramètres de configuration des mots de passe.

	90 Jours	• Effectuer un audit de suivi pour vérifier la mise en œuvre de la nouvelle politique de mots de passe et identifier tout domaine d'amélioration.
Annexes	• Rapport d'audit initial • Politique de mots de passe mise à jour • Procédure de mise à jour des mots de passe • Programme de formation sur la politique de mots de passe	

4. Lacunes dans les examens des accès des utilisateurs

Les examens des accès des utilisateurs présentent des lacunes importantes. Il est recommandé de mettre en place un processus formel d'examen périodique des accès des utilisateurs, qui doit être documenté et inclure la justification des autorisations d'accès accordées. Les chefs de département doivent identifier les activités critiques et surveiller les accès des utilisateurs pour s'assurer qu'ils sont appropriés. De plus, il est essentiel d'implémenter des contrôles d'accès basés sur le principe du moindre privilège, en accordant aux utilisateurs uniquement les autorisations nécessaires à leur travail. Enfin, il est crucial de sensibiliser les employés à l'importance de la sécurité des accès et aux dangers d'un accès non autorisé.

Responsabilités	DSI	• Élaborer et mettre en œuvre le processus d'examen des accès des utilisateurs. • Fournir des outils et des formations aux employés pour soutenir le processus d'examen.
	Chef de département	• Identifier les activités critiques et surveiller les accès des utilisateurs pour s'assurer qu'ils sont appropriés.
	Utilisateurs	• Coopérer aux tests de restauration des sauvegardes.
Calendrier	Immédiat	• Définir les exigences du processus d'examen des accès des utilisateurs. • Identifier les ressources nécessaires.
	30 Jours	• Élaborer le processus d'examen des accès des utilisateurs. • Dispenser une formation aux employés sur le nouveau processus.
	60 Jours	• Mettre en œuvre le nouveau processus d'examen des accès des utilisateurs.
	90 Jours	• Effectuer un audit de suivi pour vérifier la mise en œuvre du nouveau processus

Annexes	• Rapport d’audit initial • Procédure d’examen des accès des utilisateurs • Formulaire d’examen des accès des utilisateurs • Programme de formation sur la sécurité des accès

5. **Utilisation d'un compte utilisateur générique pour accéder à la salle des serveurs**
   L'utilisation d'un compte utilisateur générique pour accéder à la salle des serveurs pose des risques de sécurité. Il est recommandé de mettre fin à cette pratique et d'attribuer des noms d'utilisateur uniques et personnalisés à chaque individu autorisé à accéder à la salle des serveurs. Il faut exiger une authentification forte pour tous les accès, comme l'utilisation de cartes à puce ou de clés biométriques, et mettre en place des contrôles d'accès stricts pour limiter l'entrée uniquement aux personnes autorisées. L'utilisation d'un système de journalisation centralisé pour suivre tous les accès à la salle des serveurs est également conseillée. Enfin, il est crucial de sensibiliser le personnel aux risques liés à l'utilisation de comptes génériques et aux bonnes pratiques de sécurité physique.

Responsabilités	DSI	• Mettre en œuvre les recommandations techniques pour éliminer l'utilisation de comptes génériques et renforcer les contrôles d'accès à la salle des serveurs. • Fournir une formation et une sensibilisation au personnel sur les bonnes pratiques de sécurité physique.
	Direction	• Approuver et soutenir les initiatives visant à améliorer la sécurité physique de la salle des serveurs. • Allouer les ressources nécessaires à la mise en œuvre des recommandations.
	Personnel	• Respecter les nouvelles procédures de sécurité physique et utiliser des noms d'utilisateur uniques pour accéder à la salle des serveurs. • Signaler immédiatement tout accès non autorisé ou activité suspecte à la sécurité.
Calendrier	Immédiat	• Interdire l'utilisation du compte utilisateur générique "Admin_Generic_Name". • Mettre à jour les politiques de sécurité pour exiger des noms d'utilisateur uniques et une authentification forte pour l'accès à la salle des serveurs.
	30 Jours	• Mettre en œuvre un système de journalisation centralisé pour suivre tous les accès à la salle des serveurs.

		• Dispenser une formation au personnel sur les nouvelles procédures de sécurité physique.
	90 Jours	• Effectuer un audit de suivi pour vérifier la mise en œuvre des recommandations et l'efficacité des contrôles de sécurité physique.
Annexes	• Rapport d'audit initial • Politique de sécurité physique • Procédures d'accès à la salle des serveurs • Plan de formation à la sécurité physique	

6. **Politiques et procédures informatiques non mises à jour**

   Les politiques et procédures informatiques ne sont pas à jour, ce qui peut entraîner des inefficacités et des risques. Il est recommandé de mettre à jour toutes les politiques et procédures informatiques pour l'année 20XX. La fréquence d'examen des accès des utilisateurs doit être définie dans ces politiques. Il est également crucial d'assurer la cohérence entre les SLA définis dans l'outil de billetterie XYZ_Ticketting_Tool et ceux définis dans la politique. Envisager l'élaboration d'une procédure standard complète pour la gestion des politiques et procédures informatiques est conseillé. Toutes les politiques et procédures doivent obtenir l'approbation de la direction et être communiquées à tous les employés. Un processus de formation doit être mis en place pour garantir que les employés comprennent et respectent les politiques et procédures. Enfin, des audits réguliers doivent être effectués pour vérifier la mise en œuvre et l'efficacité des politiques et procédures.

Responsabilités	DSI	• Rédiger, mettre à jour et maintenir les politiques et procédures informatiques. • Obtenir l'approbation de la direction pour les politiques et procédures. • Communiquer les politiques et procédures aux employés. • Mettre en place un processus de formation. • Effectuer des audits réguliers.
	Direction	• Approuver les politiques et procédures informatiques. • Soutenir la mise en œuvre des politiques et procédures.
	Personnel	• Respecter les politiques et procédures informatiques. • Participer aux formations. • Signaler tout écart par rapport aux politiques et procédures.
Calendrier	Immédiat	• Mettre à jour les politiques et procédures qui n'ont pas été révisées pour l'année 20XX. • Définir la fréquence d'examen des accès des utilisateurs dans les politiques.

		• Assurer la cohérence entre les SLA dans l'outil de billetterie XYZ_Ticketting_Tool et les SLA définis dans la politique.
	30 Jours	• Élaborer une procédure standard complète du secteur pour la gestion des politiques et procédures informatiques. • Obtenir l'approbation de la direction pour la procédure standard.
	60 Jours	• Communiquer les politiques et procédures mises à jour à tous les employés. • Mettre en place un processus de formation.
	90 Jours	• Effectuer un audit initial pour vérifier la mise en œuvre des politiques et procédures mises à jour.
Annexes	• Rapport d'audit initial • Politiques et procédures informatiques actuelles • Procédure standard du secteur pour la gestion des politiques et procédures informatiques • Plan de formation	

7. Absence de tests de reprise après sinistre pour certaines applications critiques.

L'absence de tests de reprise après sinistre pour certaines applications critiques constitue une défaillance notable. Il est recommandé de mettre en place un plan de test DRP régulier pour l'application CORE_BAKING_SYSTEM_XYZ. Ce plan doit inclure divers scénarios de sinistre et les tests doivent être effectués au moins une fois par an. Les résultats des tests doivent être documentés et analysés, avec des actions correctives prises pour remédier à toute lacune identifiée. Il est également crucial de sensibiliser les employés à l'importance du DRP et à leurs rôles et responsabilités en cas de sinistre, ainsi que de mettre en place une formation régulière sur le DRP pour les employés.

Responsabilités	DSI	• Élaborer et mettre en œuvre le plan de test DRP. • Effectuer les tests DRP. • Documenter et analyser les résultats des tests. • Prendre des mesures correctives pour remédier aux lacunes identifiées. • Sensibiliser les employés au DRP. • Dispenser une formation DRP aux employés.
	Direction	• Approuver le plan de test DRP. • Allouer les ressources nécessaires à la mise en œuvre du plan de test DRP. • Soutenir la sensibilisation et la formation au DRP des employés.
	Personnel	• Participer aux tests DRP. • Suivre la formation DRP. • Respecter les procédures DRP en cas de sinistre.
Calendrier	Immédiat	• Élaborer le plan de test DRP. • Obtenir l'approbation de la direction pour le plan de test DRP.
	30 Jours	• Mettre en place la formation DRP pour les employés.
	60 Jours	• Effectuer le premier test DRP.
	90 Jours	• Analyser les résultats du premier test DRP et prendre des mesures correctives.

Annexes	• Rapport d'audit initial • Plan de test DRP • Procédures DRP • Programme de formation DRP

8. Lacunes dans le processus de gestion du changement

Les lacunes dans le processus de gestion du changement nécessitent des améliorations importantes. Il est recommandé de formaliser un processus de gestion du changement, en exigeant que toutes les demandes de changement soient documentées à l'aide d'un outil de suivi unique. De plus, il est essentiel de mettre en place un processus d'approbation pour les demandes de changement et de réaliser des tests UAT avant la mise en production. Il faut également obtenir des preuves d'approbation, de tests et d'acceptation des utilisateurs pour toutes les modifications apportées. Sensibiliser les employés à l'importance du processus de gestion du changement et leur fournir une formation sur ce sujet sont également des mesures essentielles à prendre.

Responsabilités	DSI	• Élaborer et mettre en œuvre le processus de gestion du changement. • Mettre en place et maintenir l'outil de suivi des demandes de changement. • Gérer le processus d'approbation des demandes de changement. • Dispenser une formation sur la gestion du changement aux employés.
	Gestionnaires métiers :	• Soumettre les demandes de changement au processus de gestion du changement. • Fournir des tests UAT pour les demandes de changement.
	Utilisateurs	• Tester les modifications du système et fournir des commentaires.
Calendrier	Immédiat	• Formaliser le processus de gestion du changement. • Sélectionner un outil de suivi des demandes de changement.
	30 Jours	• Mettre en place l'outil de suivi des demandes de changement. • Dispenser une formation sur la gestion du changement aux employés.
	60 Jours	• Mettre en œuvre le nouveau processus de gestion du changement.

	90 Jours	• Effectuer un audit de suivi pour vérifier la mise en œuvre du nouveau processus.
Annexes	• Rapport d'audit initial • Processus de gestion du changement formalisé • Procédures de gestion du changement • Programme de formation sur la gestion du changement	

9. Lacunes dans le processus de gestion des incidents

Les lacunes dans le processus de gestion des incidents nécessitent des améliorations urgentes. Il est recommandé de mettre à jour ce processus pour garantir sa conformité aux meilleures pratiques. Il est également crucial d'assurer la cohérence entre les SLA définis dans le système et la politique de l'organisation. De plus, il faut former les employés au nouveau processus de gestion des incidents afin de garantir une adoption efficace. La mise en place d'outils et de technologies pour automatiser ce processus peut grandement améliorer son efficacité. Enfin, surveiller et mesurer les performances du processus de gestion des incidents permettra d'identifier les domaines nécessitant une amélioration continue.

Responsabilités	DSI	• Élaborer et mettre à jour le processus de gestion des incidents. • Mettre en œuvre les outils et les technologies nécessaires. • Dispenser une formation aux employés. • Surveiller et mesurer les performances du processus.
	Gestionnaires métiers	• Collaborer à l'élaboration du processus de gestion des incidents. • Communiquer les SLA à leurs équipes.
	Utilisateurs	• Signaler les incidents conformément au nouveau processus. • Respecter les délais de résolution des SLA.
Calendrier	Immédiat	• Mettre à jour la politique de gestion des incidents pour qu'elle soit conforme aux meilleures pratiques. • Identifier les outils et les technologies nécessaires.
	30 Jours	• Développer un plan de formation pour les employés. • Sélectionner et mettre en œuvre les outils et les technologies.
	60 Jours	• Dispenser une formation aux employés sur le nouveau processus. • Mettre en œuvre le nouveau processus de gestion des incidents.

	90 Jours	• Effectuer un audit de suivi pour vérifier la mise en œuvre du nouveau processus.
Annexes	• Rapport d'audit initial • Politique de gestion des incidents mise à jour • Procédures de gestion des incidents • Programme de formation sur la gestion des incidents • Guide de l'utilisateur du système de gestion des incidents	

10. Déficiences dans la Surveillance des Tâches

Les déficiences dans la surveillance des tâches nécessitent des actions correctives immédiates. Il est recommandé de mettre en place un système d'alerte pour signaler les erreurs et les échecs des tâches planifiées au service informatique. Ensuite, il est crucial d'examiner les causes de ces erreurs et échecs et de prendre des mesures correctives appropriées. De plus, il faut mettre en place des procédures pour la récupération en cas de panne lors d'une erreur ou d'un échec des tâches planifiées afin de minimiser les interruptions et les perturbations.

Responsabilités	DSI	• Mettre en œuvre le système d'alerte. • Enquêter sur les causes des erreurs et des échecs des tâches planifiées. • Mettre en place des procédures de reprise après sinistre.
	Personnel de support informatique	• Répondre aux alertes et prendre les mesures appropriées
	Utilisateurs	• Signaler les erreurs et les échecs des tâches planifiées.
Calendrier	Immédiat	• Identifier les exigences du système d'alerte. • Sélectionner une solution d'alerte.
	30 Jours	• Mettre en œuvre le système d'alerte.
	60 Jours	• Examiner les causes des erreurs et des échecs des tâches planifiées. • Mettre en place des procédures de reprise après sinistre.
	90 Jours	• Effectuer un audit de suivi pour vérifier l'efficacité du système d'alerte et des procédures de reprise après sinistre.
Annexes	• Rapport d'audit initial • Exigences du système d'alerte • Spécifications de la solution d'alerte • Procédures de reprise après sinistre • Programme de test	

2.3.2 Mise en œuvre et contrôle et pilotage

La gestion des risques dans le cadre de la méthode MEHARI est un processus continu qui nécessite une mise en œuvre et un contrôle rigoureux à long terme pour être véritablement efficace. Notre étude pose les bases pour ces étapes, qui devront être poursuivies et approfondies dans un cadre opérationnel et avec des ressources adéquates.

3. Discussion

Après avoir effectué une analyse des risques par la méthode MEHARI pour trois outils essentiels au fonctionnement de la banque, nous avons relevé les conclusions suivantes :

Bien que la méthode MEHARI soit complexe et assez difficile à appliquer, comme le perçoivent Khaled Benantar, Souad Benmeziane et Omar Deghbar, elle offre néanmoins une couverture étendue des risques. Cela permet d'assurer les trois facteurs de performance DIC (Disponibilité, Intégrité et Confidentialité) du système. En outre, le type d'analyse qu'elle utilise, à savoir les échelles, permet de mieux comprendre la gravité et l'impact des risques ce qui est conclu par Amanda Wanderley qui met en avant le rôle essentiel de ces échelles pour fournir une évaluation objective de la gravité potentielle des risques, qu'ils soient positifs ou négatifs. En évaluant la gravité des risques, les entreprises peuvent hiérarchiser leur gestion en fonction de leur criticité, ce qui permet une prise de décision plus éclairée et proactive.

Notre étude confirme la perception de Bowen et al. qui affirment que la gestion des risques est un élément essentiel pour assurer la gouvernance IT. Les risques identifiés dans les outils, qu'ils soient métiers ou bien de support, lors de la mission d'audit IT, ont un impact significatif sur l'existence des organisations. Ces derniers peuvent être destructeurs pour l'organisation, déclenchant des crises graves, entraînant des dommages à la réputation, des pertes financières et des responsabilités légales, d'où la nécessité de l'audit de la gestion des risques.

Pour faire face à ces risques, il est essentiel de non seulement corriger les vulnérabilités du système, mais aussi de sensibiliser le personnel à ces enjeux. Ces deux facteurs doivent être pris en compte conjointement, car l'un sans l'autre reste inutile. Cela a été abordé dans le webinaire du 8 juin 2022 entre l'École Supérieure d'Informatique (ESI) et Optimum Télécom Algérie, dirigé par le Professeur Ghomari A.R., qui a souligné l'importance de l'implication et de la collaboration des employés dans les projets informatiques pour réduire les risques et améliorer la résilience de l'entreprise face aux menaces technologiques émergentes. L'article de l'Institute of Internal Auditors corrobore cette approche, affirmant que la réussite de la gestion des risques repose sur la collaboration entre le personnel et les mesures de sécurité technique.

Nos résultats d’audit confirment également les résultats de la recherche menée par Calder et al., qui soulignent la nécessité de valider et de gérer correctement les risques de manière continue à travers des audit interne. Nos résultats suggèrent la mise en place de contrôles pour identifier et éliminer les causes potentielles des problèmes, ainsi que pour surveiller les événements déclencheurs afin d'atténuer leurs effets. Cela passe par des activités d’audit interne de manière continue, permettant ainsi de réussir un axe de la gouvernance IT qui est la gestion des risques.

CONCLUSION

L’objectif de cette recherche était d’approfondir les compréhensions de la gouvernance des technologies de l'information ainsi que du rôle de l'audit IT, ainsi que méthodes pouvant être déployées en mission d'audit. Nous nous sommes également penchés sur les pratiques actuelles de KPMG dans ce domaine. Ainsi que de contribuer à l'amélioration des pratiques d’audit de KPMG et à renforcer leur position en tant que leader dans le domaine de l'audit et du conseil.

Pour ce faire, nous avons adopté une approche qualitative en réalisant des entretiens avec trois responsables impliqués dans la mission étudiée, afin de répondre à notre besoin d’identifier et de traiter les risques liés au client.

Nos résultats nous ont permis de mieux évaluer le client en obtenant une vision plus détaillée de leurs risques. Les résultats de notre recherche confirment l’effet positif de la méthode MEHARI sur la gestion des risques. Notons que MEHARI est une méthode peu utilisée dans le domaine de l'audit IT, les cabinets se concentrant davantage sur les normes et référentiels existants. Cependant, MEHARI demeure une méthode plus détaillée et structurée, basée sur les normes ISO 27001 et ISO 27002.

Il est également important de souligner que cette recherche est la première étude scientifique réalisée chez KPMG et, à notre connaissance, très peu étudiée en Algérie. Ainsi, sur le plan managérial, nos résultats sont encourageants pour KPMG, mais aussi pour les clients, qui bénéficient d’une meilleure assurance de leur environnement IT.

Nous suggérons donc au cabinet de réexaminer cette méthode avec des experts du domaine et d’envisager son intégration dans leur démarche d’audit auprès de leurs clients.

Comme toute recherche, notre travail comporte des limites, dont la plus importante est le périmètre restreint de notre étude de cas. Celle-ci se limite à l'application d'une seule méthode sur trois actifs. De plus, il existe un manque de littérature sur l’application spécifique de cette méthode. Par ailleurs, la mise en œuvre et le contrôle des mesures de sécurité n'ont pas pu être réalisés en raison des contraintes temporelles et des ressources limitées. Ces étapes sont cependant essentielles pour garantir une gestion efficace et durable des risques.

Pour des travaux futurs, il serait intéressant de prolonger l'étude sur plusieurs mois ou années afin d'inclure ces étapes. Cela permettrait de valider l'efficacité des mesures recommandées et

de développer une stratégie de gestion des risques plus complète et adaptable aux évolutions des menaces. Il serait également pertinent d'étudier d'autres méthodes et d’élargir le périmètre de l'analyse pour mieux évaluer les systèmes et offrir une assurance significative.

RÉFÉRENCES BIBLIOGRAPHIQUES

Articles

- Benantar, Khaled, Benmeziane, Souad, et Deghbar, Omar. "Étude comparative des méthodes de gestion des risques : MEHARI, Ebios et Octave." Publié en 2023.
- Bowen, et al. "IT Governance and Risk Management." 2007.
- Clusif (Club des Utilisateurs de la Sécurité des Systèmes d'Information). "Définition de la sécurité des systèmes d'information."
- Ernst & Young. "Un processus continu et intégré de gestion des risques." 2022.
- FERMA. "CADRE DE RÉFÉRENCE DE LA GESTION DES RISQUES." 2011.
- Guibert, 2007. Source pour la Figure 1: Le modèle opérant, information et décision.
- Helmi, Driss, et Kaya, Kamel. "Améliorer la performance des PME en intégrant l'intelligence artificielle." Publié en 2023.
- Howard, 2023. "Objectifs de la gouvernance IT."
- Hughes, M. "The impact of IT failures on business continuity." 2006.
- Institute of Internal Auditors (IIA). "Prise de position de l'IIA: Les trois lignes de maîtrise pour une gestion des risques et un contrôle efficaces." Janvier 2013.
- Kroenke, David M., et Mesaglio, Michael. "Définition du système d'information." 2010.
- Mohamed, Abdelouahed, et Gaid Noureddine, Ahmed. "Contribution de l'audit dans la gestion des risques liés aux systèmes d'information dans le cadre de la gouvernance des systèmes d'information - Cas Evolutec International – Algérie." 2017.
- Rimol, 2022. "L'importance de la gouvernance IT."
- Trautmann, Triche, et Wetherbe. "System Failures and Risk Management in IT." 2013.
- Wanderley, Amanda. "Comment construire des échelles de cotation des risques." Publié en 2023.
- Wanderley, Amanda. "Qu'est-ce que la gestion des risques ?" Publié en 2023.

Ouvrages

- Abdelmalek, Sadok, et al. "La gouvernance IT : Structures et processus de leadership." 2020.
- CMMI Institute. "CMMI Development and Implementation Guide".
- Guide ISO 31000:2018. "Management du risque – Lignes directrices".
- ISACA. "COBIT 2019 Framework."
- Maizlish, B., et Handler, R. "IT Portfolio Management: Unlocking the Business Value of Technology." 2005.
- Manuel ITIL v4. "Gestion des services informatiques et infrastructure IT".

- Nejib Salhi. "Audit et analyse des risques de la sécurité du système d'information ; Methodologie : PSC/ISO 27002 et MEHARI." 2015.
- Weill, P., et Ross, J. W. "IT Governance: How Top Performers Manage IT Decision Rights for Superior Results." 2004.

Thèses

- **Huang, et al. "Enterprise Risk Management in IT Governance." 2011.**
- Uky Yudatama, Bobby Nazief, Achmad Nizar Hidayanto. "Les cinq axes de la gouvernance IT." 2017.
- Van Grimbergen, et al. "Creating IT Value through Risk Management." 2004.
- Wallace, Keil, et Rai. "A Framework for Managing IT Risks." 2004.

Webinar

- Ghomari, A.R. "Webinaire entre l'École Supérieure d'Informatique (ESI) et Optimum Télécom Algérie, sur la gestion des systèmes informatiques." 8 juin 2022.
- ISACA. "Excellence en Gouvernance des Technologies de l'Information (EGIT)." 2020.
- ITGI (IT Governance Institute). "La gouvernance des technologies de l'information (IT)." 2006.
- Morisse, 2019. "Les activités de la gouvernance : Surveiller, Évaluer, Diriger."

Normes et Référentiels

- AFNOR (2016). "L'effet de l'incertitude sur des objectifs". Norme de définition du risque.
- Framework COBIT2019
- ISA 315 Revised. "Identifying and Assessing the Risks of Material Misstatement."
- ISO 19011 (2018). "Lignes directrices pour l'audit des systèmes de management".
- ISO 31000 (2018). "Management du risque – Principes et lignes directrices".
- ISO 2700X. Norme internationale pour la sécurité de l'information.
- ITIL V4
- CLUSIF (Club de la Sécurité de l'Information Français). "Méthodologie MEHARI".

ANNEXE A –GUIDES D'ENTRETIEN

Guide d'entretien N°1

(destiné aux auditeurs)

Thème 01 : renseignements

- Pourriez-vous nous fournir votre nom, prénom et votre âge ?
- Quel est votre poste ou titre au sein de l'organisation ?
- Depuis combien de temps occupez-vous ce poste ?
- Pourriez-vous nous décrire brièvement vos responsabilités et principales missions au sein de l'organisation ?

Thème 02 : Gestion des accès

1. Authentification

- Comment les utilisateurs s'authentifient-ils pour accéder aux applications bancaires ?
- Y a-t-il des mesures en place pour empêcher l'utilisation des identifiants d'autres utilisateurs ?
- Quelles sont les politiques de mot de passe en place pour les applications et les systèmes d'exploitation (par exemple, longueur minimale, complexité, expiration) ?
- Comment assurez-vous que les paramètres de verrouillage de compte sont configurés pour se conformer aux meilleures pratiques et normes de l'industrie ?
- Quelles mesures sont prises pour surveiller et détecter les tentatives de connexion non autorisées ?

2. Autorisation

- Quels sont les contrôles pour garantir que les utilisateurs n'ont accès qu'aux informations nécessaires pour leur poste ?
- Comment la séparation des tâches est-elle assurée et vérifiée ?
- Comment les accès des utilisateurs sont-ils revus et approuvés périodiquement pour garantir leur conformité avec les exigences de sécurité ?
- Quels mécanismes existent pour auditer et vérifier les accès des utilisateurs à des intervalles réguliers ?

3. Attribution

- Quels processus existent pour l'attribution des droits d'accès aux nouveaux utilisateurs ?
- Comment les modifications des privilèges d'accès des utilisateurs existants sont-elles gérées et autorisées ?

4. Révocation

- Comment les droits d'accès sont-ils révoqués lorsqu'un utilisateur quitte l'entreprise ou change de poste ?
- Quels délais sont appliqués pour révoquer les accès après la cessation de l'emploi ?
- Quels mécanismes sont en place pour s'assurer que les droits d'accès des utilisateurs partants sont révoqués avant ou immédiatement après leur dernier jour de travail ?
- Quels sont les contrôles en place pour vérifier qu'il n'y a pas de retard dans la désactivation des accès des utilisateurs et es ce que ces contrôles sont documentés ?

5. **Accès privilégié**

- Comment les droits d'administrateur ou les droits avec pouvoirs sont-ils attribués et contrôlés ?
- Y a-t-il des audits réguliers des comptes à privilèges élevés ?

6. **Examen des accès utilisateurs**

- À quelle fréquence les accès utilisateurs sont-ils examinés ?
- Quels processus sont en place pour rectifier les anomalies détectées lors des examens des accès ?
- Comment les revues périodiques des accès des utilisateurs sont-elles documentées et suivies ?
- Qui est responsable de l'exécution et de la validation des revues des accès des utilisateurs ?
- Quels contrôles sont en place pour s'assurer que les utilisateurs n'ont accès qu'aux informations nécessaires pour leur poste ?
- Comment les changements dans les droits d'accès des utilisateurs sont-ils communiqués et mis en œuvre ?

7. **Paramètres de sécurité**

- Quels paramètres de sécurité sont configurés sur les technologies utilisées ?
- Comment ces paramètres sont-ils alignés avec les normes de l'entreprise ?
- Comment assurez-vous que les politiques de mot de passe sont régulièrement mises à jour et conformes aux meilleures pratiques ?
- Quels mécanismes sont en place pour identifier et corriger les exceptions aux politiques de mot de passe ?

8. **Politiques et procédures**

- Les politiques et procédures de gestion des accès sont-elles révisées et mises à jour régulièrement ?
- À quelle fréquence les revues d'accès des utilisateurs sont-elles définies dans les politiques et procédures ?

9. **Accès physique**

- Quels contrôles sont en place pour restreindre l'accès physique aux centres de données et au matériel informatique ?
- Comment l'accès physique est-il surveillé et enregistré ?
- Y a-t-il des comptes utilisateurs génériques utilisés pour accéder aux centres de données ou aux salles des serveurs ? Si oui, comment sont-ils gérés et surveillés ?
- Quels processus sont en place pour attribuer des identifiants uniques et personnalisés aux utilisateurs ayant accès aux zones sensibles ?
- Comment assurez-vous que chaque accès physique est traçable à un individu spécifique pour améliorer la responsabilité individuelle ?
- Quelles mesures sont prises pour désactiver ou remplacer les accès génériques existants ?
  - Comment la conformité des accès physiques est-elle vérifiée et audité régulièrement ?

Thème 03 : Gestion des incidents

- Quel est le processus formel pour identifier, documenter, et prioriser les incidents dans les systèmes ?
- Comment assurez-vous que les incidents sont résolus conformément aux priorités définies et aux SLA établis ?
- Quelles sont les mesures en place pour gérer les incidents qui nécessitent une analyse approfondie ou des corrections complexes qui pourraient dépasser les délais définis par les SLA ?
- Quel est le processus pour traiter les incidents liés aux erreurs ou aux échecs des tâches planifiées ?
- Comment assurez-vous une communication efficace entre les utilisateurs métier et le département informatique en cas d'erreur ou d'échec des tâches planifiées ?

Thème 04 : Gestion des changements

1. Politique et procédure

- Les politiques et procédures de gestion des changements sont-elles alignées avec les pratiques actuelles et révisées périodiquement ?
- Comment assurez-vous que les SLA définis dans les politiques sont cohérents avec ceux implémentés dans les outils de gestion des tickets ?

2. Processus de gestion des changements

- Quel est le processus pour la conception, la programmation, et la mise à l'essai des changements dans les applications bancaires ?
- Comment les changements sont-ils intégrés à l'environnement de production ?
- Quel est le processus formel pour documenter, autoriser, tester et approuver les changements dans le système?
- Comment assurez-vous que tous les changements sont enregistrés de manière cohérente et centralisée ?
- Quelles mesures sont prises pour garantir que les demandes de changement ne sont pas laissées ouvertes après leur mise en production ?

3. Séparation des tâches dans le cadre de l'intégration des changements

- Comment la séparation des droits d'accès pour l'apport de changements et leur intégration est-elle assurée ?
- Qui est responsable de vérifier cette séparation ?

4. Élaboration, acquisition ou mise en œuvre des systèmes

- Quels contrôles sont en place lors de l'élaboration ou de la mise en œuvre initiale des applications informatiques ?
- Comment les nouvelles applications sont-elles testées avant d'être mises en production ?

5. Conversion des données

- Comment les données sont-elles converties lors de la mise en œuvre ou des mises à niveau des systèmes ?
- Quels contrôles sont en place pour vérifier l'exactitude et l'intégrité des données converties ?

Thème 05 : Gestion des opérations informatiques

1. Politique et procédures

- Les politiques de sauvegarde et de récupération des données sont-elles révisées et mises à jour régulièrement ?
- Les politiques et procédures en matière de détection des intrusions sont-elles conformes aux normes actuelles et revues périodiquement ?

2. Planification des travaux

- Comment les travaux ou programmes pouvant avoir une incidence sur l'information financière sont-ils planifiés et lancés ?
- Quels sont les processus pour assurer que ces travaux sont correctement exécutés ?

3. Suivi des travaux

- Comment le suivi des travaux ou programmes portant sur l'information financière est-il assuré ?
- Y a-t-il des mécanismes de contrôle pour détecter et corriger les erreurs durant ces travaux ?
- Comment les incidents sont-ils suivis et résolus conformément aux accords de niveau de service (SLA) définis ?
- Quelles sont les procédures en place pour assurer que les priorités des incidents sont correctement assignées ?
- Comment gérez-vous les écarts entre les SLA définis dans le système et ceux documentés dans la politique organisationnelle ?
- Quel est le processus actuel pour surveiller les tâches planifiées?
- Les alertes sont-elles configurées pour être déclenchées en cas d'erreurs ou d'échecs des tâches planifiées ?
- Comment sont gérées les notifications d'erreurs ou d'échecs de tâches ?
- Quels sont les plans de reprise après sinistre (DRP) en place et comment sont-ils testés ?
- Comment assurez-vous que les interconnexions et les interdépendances entre les différentes applications et plateformes sont couvertes dans les tests de reprise après sinistre ?

4. Sauvegarde et récupération

- Quelle est la fréquence des tests de reprise après sinistre (DRP)?
- Comment les résultats des tests de reprise après sinistre sont-ils documentés et évalués ?
- Les employés sont-ils formés et conscients de leurs responsabilités en cas de désastre ? Comment cette formation est-elle mise à jour et testée ?

5. Détection des intrusions

- Quels sont les systèmes de détection d'intrusions en place ?
- Comment les points vulnérables de l'environnement informatique sont-ils surveillés et corrigés ?

Guide d'entretien N°2

(destiné à la DSI de la banque)

Questions pour l'application SWIFT

1. **Utilité de l'application :**

- À quoi sert cette application ?

2. **Évaluation de la criticité (échelle de 1 à 4) :**

- À quel point la non-disponibilité, la non-intégrité et la non-conformité des couches applicative, base de données et système d'exploitation sont-elles graves ?

3. **Processus métier et support :**

- Quels sont les processus métier et support de cet outil ?

4. **Criticité des processus (échelle de 1 à 4) :**

- À quel point la non-disponibilité, la non-intégrité et la non-conformité de ces processus sont-elles graves ?

			D	I	C
SWIFT	Couche	APP			
		BDD			
		OS			
	Processus métier				
	Processus support				

Questions pour l'application Core Banking System

1. **Utilité de l'application :**

- À quoi sert cette application ?

2. **Évaluation de la criticité (échelle de 1 à 4) :**

- À quel point la non-disponibilité, la non-intégrité et la non-conformité des couches applicative, base de données et système d'exploitation sont-elles graves ?

3. **Processus métier et support :**

- Quels sont les processus métier et support de cet outil ?

4. **Criticité des processus (échelle de 1 à 4) :**

- À quel point la non-disponibilité, la non-intégrité et la non-conformité de ces processus sont-elles graves ?

			D	I	C
Core Banking system application	**Couche**	**APP**			
		BDD			
		OS			
	Processus métier				
	Processus support				

Questions pour les applications Service Desk et ITSM

1. **Utilité des applications :**

- À quoi servent ces applications ?

2. **Évaluation de la criticité (échelle de 1 à 4) :**

- À quel point la non-disponibilité, la non-intégrité et la non-conformité des couches applicative, base de données et système d'exploitation sont-elles graves ?

3. **Processus métier et support :**

- Quels sont les processus métier et support de ces outils ?

4. **Criticité des processus (échelle de 1 à 4) :**

- À quel point la non-disponibilité, la non-intégrité et la non-conformité de ces processus sont-elles graves ?

			D	I	C
Service desk application / ITSM application	**Couche**	**APP**			
		BDD			
		OS			
	Processus métier				
	Processus support				

GRILLE D'ANALYSE

Grille de l'entretient N°01

Thèmes	Catégories	Verbatim de l'auditeur 01	Verbatim de l'auditeur 02	Verbatim de l'auditeur 03
Gestion des accès	**Authentification**	« Les utilisateurs s'authentifient principalement avec un nom d'utilisateur et un mot de passe. Le problème c'est qu'on a constaté que les politiques de mot de passe ne sont pas toujours conformes, avec des configurations souvent trop simples. » « Ils prévoient des mots de passe avec une longueur minimale et une certaine complexité. Pour l'application CORE_BAKING_SYSTEM, le nombre d'échecs de connexion avant le verrouillage du compte est bien supérieur. »	« Même s'il y a des politiques pour empêcher l'utilisation des identifiants d'autres utilisateurs, on a découvert que des comptes génériques étaient encore utilisés pour l'accès aux salles de serveurs, ce qui prouve qu'ils ne sont pas appliqués. »	« On a constaté que les paramètres de verrouillage de compte ne sont pas systématiquement configurés. Par exemple, la durée de verrouillage de compte n'était pas configurée sur certains systèmes. » « Il y'a des mécanismes de surveillance, mais ils ne sont pas toujours efficaces. Les tentatives de connexion non autorisées sont pas systématiquement détectées et traitées. »
	Autorisation	« Des contrôles existent, oui, mais ils ne sont pas sérieusement appliqués. L'audit a révélé que les revues d'accès utilisateur ne sont pas fait de façon régulière, ce qui permet à certains utilisateurs de conserver des droits d'accès non nécessaires. »	« La séparation des tâches n'est pas toujours respectée. Il manque des revues régulières pour s'assurer que les tâches critiques sont bien séparées entre différents utilisateurs. »	« La revue périodique des accès utilisateur est une procédure qui est censée être en place, mais ces revues ne sont pas systématiques. Cela crée un risque de non-conformité. » « Les audits des accès utilisateurs sont effectués, mais ils ne sont pas fréquents et manquent de rigueur. Y'a des anomalies qui sont identifié qu'a l'audit suivant. »
	Attribution	« Il y'a un processus formel pour l'attribution		« Les modifications des privilèges d'accès sont

		des droits d'accès, mais il est souvent retardé par des procédures bureaucratiques. Les nouveaux utilisateurs peuvent attendre plusieurs jours avant d'obtenir les accès nécessaires. »		censées être approuvées par les responsables, mais il y a des retards et des manques de documentation. Ça peut entraîner des utilisateurs ayant des privilèges »
	Révocation	« Les droits d'accès sont révoqués par les RH ou le gestionnaire direct, mais on a relevé des retards significatifs dans plusieurs cas, certains accès étant révoqués plusieurs jours après le départ de l'utilisateur. »	« Les délais sont censés être immédiats, mais y'en a qui peuvent aller jusqu'à plusieurs semaines. » « Il y a un suivi, mais il n'est pas efficace. Des cas de retards dans la révocation des accès ont été documentés. »	« Les contrôles sont partiellement en place, mais ils manquent de documentation et de rigueur, ce qui permet des retards dans la désactivation des accès. »
	Accès privilégié	« Les droits d'administrateur sont attribués par les responsables IT, mais le suivi et le contrôle sont insuffisants. »	« Les audits des comptes à privilèges élevés ne sont pas menés de manière régulière, ce qui laisse des lacunes dans la surveillance des accès critiques »	
	Examen des accès utilisateurs	« Les examens sur les accès utilisateurs ne sont pas fait régulièrement. Cela a conduit à des utilisateurs ayant des accès non nécessaires à leurs fonctions » « Les changements dans les droits d'accès sont communiqués via un système de ticketing, mais il y a souvent des retards dans la mise en œuvre des modifications »	« Les anomalies détectées sont rectifiées tardivement, par ce qu'il n'y a pas de processus clair et rapide pour corriger les problèmes identifiés. »	« La documentation et le suivi des revues périodiques des accès sont insuffisants. Il manque souvent des preuves qu'ils ont été effectués, ce qui complique le suivi et la conformité. » « Les contrôles ne sont pas suffisamment rigoureux ni fréquemment vérifiés, ce qui permets à certains utilisateurs d'accéder à des informations pas nécessaires à leur poste. »
	Paramètres de sécurité	« Les politiques de mot de passe ne sont pas régulièrement mises à	« Les paramètres de sécurité ne sont pas toujours alignés avec les	« Les paramètres de sécurité configurés sont souvent en dessous des standards. »

		jour. On a détecté plusieurs faiblesses dans les configurations de mot de passe actuelles. »	normes de l'entreprise, entraînant des incohérences et des risques de sécurité. »	« Les mécanismes pour identifier et corriger les exceptions ne sont pas appliqués, ce qui permet des dérogations non contrôlées aux politiques de mot de passe. »
	Politiques et procédures	« Les politiques et procédures ne sont pas révisées et mises à jour régulièrement »	« La communication et l'application sont insuffisantes, lors de notre audit de nombreux employés n'étaient pas au courant des politiques de sécurité actuelles. »	« La formation des utilisateurs est inadéquate. Les programmes de formation ne sont pas régulièrement mis à jour. »
	Accès physique	« L'accès est principalement contrôlé par des cartes d'accès électroniques, mais on a noté que des utilisateurs non autorisés peuvent parfois accéder aux zones sensibles et que les vérifications manuelles sont rarement effectuées. » « L'accès physique est surveillé par un système de caméra de surveillance 24/7, et les enregistrements d'accès sont conservés dans un journal électronique. Mais, la revue de ces journaux n'est pas effectuée régulièrement, et des anomalies passent inaperçues. En plus, les systèmes de surveillance manquent de redondance » « La conformité des accès physiques est censée être	« Oui, des comptes utilisateurs génériques sont utilisés pour accéder aux centres de données et aux salles des serveurs. Ils sont censés être temporaires et uniquement en cas d'urgence, mais il n'y a pas de suivi des activités associées à ces comptes. Ça représente un risque majeur pour la sécurité, car il devient difficile de tracer les actions spécifiques à un individu. » « La conformité des accès physiques est censée être vérifiée par des audits internes réguliers, mais en réalité, ces audits sont souvent superficiels. Il n'existe pas de calendrier pour ces vérifications. »	« En théorie, des processus existent pour attribuer des identifiants uniques et personnalisés, mais leur mise en œuvre laisse à désirer. Les procédures sont mal définies et souvent non respectées. Il y a aussi des retards dans l'activation et la désactivation de ces identifiants, et de nombreux utilisateurs conservent leurs accès bien après avoir quitté leurs fonctions. » « Les systèmes de journalisation des accès manquent de robustesse et ne sont pas audités ce qui rend la traçabilité difficile à garantir. »

		vérifiée par des audits internes réguliers, mais en réalité, ces audits sont souvent superficiels. Il n'existe pas de calendrier pour ces vérifications. »		
Gestion des incidents (continuité)	**Gestion des incidents**	« On a identifié des lacunes dans le processus de gestion des incidents. Bien qu'il y ait un processus pour signaler les incidents. Ils sont pas toujours documentés. En plus, il y a un manque de définition claire des priorités pour les incidents, ce qui entraîne des retards dans la résolution des incidents. » « Les processus actuels ne sont pas prévue pour gérer les incidents qui exigent une analyse approfondie ou des corrections complexes. Ce qui entraîner des retards dans la résolution des incidents. »	« Les incidents ne sont pas résolus conformément aux SLA établis.la gestion des priorités est souvent négligée, ce qui signifie que des incidents critiques peuvent être relégués au second plan. » « La communication entre les utilisateurs métier et le département informatique en cas d'erreur ou d'échec des tâches planifiées est actuellement insuffisante. Il n'y a pas de mécanisme clair pour que les utilisateurs signalent ces problèmes. »	« Le processus pour traiter les incidents liés aux erreurs ou aux échecs des tâches planifiées est mal défini. Les alertes ne sont pas toujours configurées pour ces incidents, ce qui signifie que les erreurs peuvent passer inaperçues jusqu'à ce qu'elles causent des problèmes plus graves. »
Gestion des changements	**Politiques et procédures**	« Certaines politiques de gestion des changements ne sont pas révisées régulièrement. Du coup, il y a un décalage entre les pratiques actuelles et les documents de référence. »	« On a trouvé que les SLA dans les politiques ne correspondent pas toujours à ceux dans l'outil de gestion des tickets XYZ_Ticketting_Tool. »	« Certaines politiques de gestion des changements stagnent sans révision régulière, ce qui crée un écart entre les pratiques en vigueur et les documents de référence. On a eu ce constat après la découverte que les SLA définis dans ces politiques ne concordent pas avec ceux intégrés dans l'outil de gestion des tickets XYZ_Ticketing_Tool. »

	Processus de gestion des changements	« La documentation et l'approbation des changements sont incomplètes. Certains changements ne sont pas correctement testés ou autorisés avant d'être mis en production, comme on l'a vu avec CORE_BAKING_SYSTEM_XYZ. » « On a vu des demandes de changement rester ouvertes même après leur mise en production. »	« Les changements devraient être intégrés après avoir été documentés, testés et approuvés. Pourtant, on a trouvé des cas où les tests d'acceptation utilisateur ont été faits après la mise en production »	« Certains changements n'ont pas de preuves d'approbation ou de tests, ce qui remet en question l'intégrité et la sécurité des modifications. » « Actuellement, les changements sont enregistrés à travers plusieurs outils différents (Project_Management_Software_XYZ, XYZ_Ticketting_Tool et emails), ce qui disperse les informations et complique le suivi. »
	Séparation des tâches dans l'intégration des changements	« Théoriquement, la séparation des tâches est assurée par des contrôles d'accès spécifiques, mais en pratique, il y a des manquements où les mêmes utilisateurs peuvent initier et intégrer des changements sans contrôle adéquat. »	« L'équipe de sécurité informatique est responsable de cette vérification. »	« Il y a des lacunes dans la supervision et le contrôle, permettant des accès et modifications non autorisés. »
	Élaboration, acquisition ou mise en œuvre des systèmes	« Les contrôles mais ne sont pas appliqués. Par exemple, les tests de récupération après sinistre (DRP) pour des applications critiques comme CORE_BAKING_SYSTEM_XYZ n'ont pas été faits.»	« Les nouvelles applications sont censées être testées dans un environnement de préproduction. mais, des cas de mise en production sans tests adéquats ont été observés, compromettant la stabilité et la sécurité des systèmes. »	
	Conversion des données	« La conversion des données est généralement bien planifiée, mais les contrôles pour vérifier l'exactitude et l'intégrité des données converties		« Les contrôles existent, mais sont insuffisamment appliqués. Par exemple, il n'y a pas de documentation systématique des résultats des tests de conversion de

		manquent souvent de rigueur. Cela peut entraîner des erreurs et des dysfonctionnements dans les applications mises à jour. »		données, rendant la vérification des données post-conversion quasi impossible.»
Gestion des opérations informatiques	**Politiques et procédures**	« Non. Bien que la politique stipule des révisions régulières, nous avons constaté que les tests de restauration de sauvegarde ne sont pas effectués mensuellement comme prévu. » « Les résultats des tests ne sont pas documentés »	« Pas complètement. Bien que des systèmes de détection d'intrusions soient en place, nous avons identifié des lacunes dans la surveillance et la correction des vulnérabilités »	
	Planification des travaux	« La planification des travaux se fait de manière ad hoc, souvent sans documentation formelle adéquate. » « Traîne des incohérences dans le suivi et l'approbation. »	« Les changements sont parfois initiés par différents moyens comme des e-mails, outils de ticketing ex... Ce qui entraîne des incohérences dans le suivi et l'approbation. »	« Les processus sont insuffisamment rigoureux. » « Des changements sont parfois mis en production sans tests utilisateurs approprié » « Des erreurs non détectées avant la mise en service. »
	Suivi des travaux	« Le suivi est principalement réactif. Il n'y a pas de mécanisme de contrôle automatisé en place pour détecter et corriger les erreurs en temps réel » « Les problèmes sont souvent signalés par les utilisateurs finaux. » « Il n'y a pas de processus clair pour gérer ces écarts, ce qui conduit à des incohérences dans la gestion des incidents. » « Les alertes ne sont pas configurées, ce qui	« Non, les alertes ne sont pas configurées pour être déclenchées en cas d'erreurs ou d'échecs des tâches planifiées. » « Identification tardive des problèmes. » « Il n'existe pas de mécanisme de surveillance proactive. Les tâches sont surveillées manuellement, ce qui est inefficace et sujet aux erreurs. »	« Les incidents ne sont pas toujours résolus dans les délais définis par les SLA. » « Il y a une divergence entre les SLA documentés dans les politiques et ceux utilisés dans le système de gestion des tickets. » « Les priorités ne sont pas toujours définies de manière appropriée, ce qui entraîne des retards dans la résolution des incidents critiques. »

		signifie que les erreurs ne sont souvent détectées que lorsque les utilisateurs en informent l'IT. » « Les notifications d'erreurs sont principalement gérées de manière réactive par les utilisateurs finaux »		
	Sauvegarde et récupération	« Les tests de reprise après sinistre ne sont pas effectués régulièrement. » « Pas de documentation DRP ce qui complique l'évaluation de l'efficacité du plan de reprise après sinistre » « Aucune assurance ou garantie pour la reprise »	« Pour le système CORE_BAKING_SYSTEM_XYZ, aucun test de DRP n'a été réalisé récemment. » « Il n'y a pas de documentation systématique des résultats des tests »	« Il existe des applications qui n'ont aucun test DRP » « Ainsi que l'absence de documentation des résultats des tests »

Grille de l'entretient N°02

<table>
<tr><th>Thème</th><th>Sujet</th><th>Réponse</th></tr>
<tr><td rowspan="5">SWIFT</td><td>Utilité de l'application</td><td>« utilisée pour effectuer des transactions financières internationales »
« et des échanges sécurisés de messages financiers entre banques et institutions financières à travers le monde. »</td></tr>
<tr><td>Évaluation de la criticité par couche</td><td>« essentielle pour les opérations financières de la banque »
« Toute interruption, corruption de données ou faille de sécurité peut entraîner des pertes financières significatives, des sanctions réglementaires et une perte de confiance de la part des clients et des partenaires »
(Réponses sur tableau)</td></tr>
<tr><td>Processus métier et support</td><td>« Les processus métier supportés par SWIFT incluent la gestion des paiements internationaux, les virements bancaires, les échanges de devises et les transferts de fonds entre institutions financières, Messagerie financière, Surveillance des transactions et conformité réglementaire. »
« Le support comprend Gestion des clés de sécurité, développement technologique, Gestion des membres, Gestion de la Continuité des Services, Gestion des Changements, Gestion des Problèmes, Gestion des Incidents, Gestion de la configuration et Gestion des demandes de service »</td></tr>
<tr><td>Criticité des processus</td><td>« Les processus métier gérés par SWIFT sont vitaux pour les opérations financières de la banque »
« processus de support sont également cruciales pour assurer la continuité des opérations et la sécurité des informations échangées »</td></tr>
<tr><td></td><td>
<table>
<tr><th></th><th></th><th></th><th>D</th><th>I</th><th>C</th></tr>
<tr><td rowspan="18">SWIFT</td><td rowspan="3">Couche</td><td>APP</td><td>4</td><td>4</td><td>4</td></tr>
<tr><td>BDD</td><td>4</td><td>4</td><td>4</td></tr>
<tr><td>OS</td><td>4</td><td>4</td><td>4</td></tr>
<tr><td rowspan="6">Processus métier</td><td>Gestion des paiements</td><td>4</td><td>4</td><td>4</td></tr>
<tr><td>les virements</td><td>4</td><td>4</td><td>4</td></tr>
<tr><td>échanges de devises</td><td>4</td><td>4</td><td>4</td></tr>
<tr><td>Messagerie financière</td><td>4</td><td>4</td><td>4</td></tr>
<tr><td>Surveillance des transactions</td><td>4</td><td>4</td><td>4</td></tr>
<tr><td>Conformité réglementaire</td><td>4</td><td>4</td><td>4</td></tr>
<tr><td rowspan="8">Processus support</td><td>Gestion des clés de sécurité</td><td>4</td><td>4</td><td>4</td></tr>
<tr><td>Développement technologique</td><td>2</td><td>3</td><td>3</td></tr>
<tr><td>Gestion des membres</td><td>4</td><td>3</td><td>3</td></tr>
<tr><td>Gestion de la Continuité des IT</td><td>4</td><td>4</td><td>4</td></tr>
<tr><td>Gestion des Changements</td><td>4</td><td>4</td><td>4</td></tr>
<tr><td>Gestion des Problèmes</td><td>4</td><td>4</td><td>4</td></tr>
<tr><td>Gestion des Incidents</td><td>4</td><td>4</td><td>4</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td></td><td colspan="5"><table>
<tr><td></td><td></td><td>Gestion de la configuration</td><td>4</td><td>4</td><td>4</td></tr>
<tr><td></td><td></td><td>Gestion des demandes de service</td><td>4</td><td>4</td><td>4</td></tr>
</table></td></tr>
<tr><td rowspan="5">Core Banking System</td><td>Utilité de l'application</td><td colspan="5">« utilisée pour gérer les opérations bancaires de base, y compris la gestion des comptes clients, les transactions financières, les prêts, les dépôts et les services de paiements »
« Elle est le cœur des activités bancaires . »</td></tr>
<tr><td>Évaluation de la criticité par couche</td><td colspan="5">« vitale pour les opérations bancaires quotidiennes. »
« Toute interruption, perte d'intégrité des données ou non-conformité aux normes de sécurité peut entraîner des perturbations significatives »
« des pertes financières, des risques de conformité réglementaire et une perte de confiance de la clientèle »
(Réponses sur tableau)</td></tr>
<tr><td>Processus métier et support</td><td colspan="5">« Les processus métier supportés par le Core Banking System incluent la Rapport financier, gestion des comptes clients, le traitement des transactions, la gestion des prêts et crédits, les services de paiement, Provision pour pertes sur créances, Trésorerie, et le traitement des dépôts et retraits»
« Le support tout comme Swift inclut la maintenance des systèmes, la gestion des incidents, les mises à jour de sécurité… »</td></tr>
<tr><td>Criticité des processus</td><td colspan="5">« Les processus métier gérés par le Core Banking System sont cruciaux pour les opérations bancaires. »
« processus de support sont tout aussi critiques pour garantir une opération fluide et sécurisée du système bancaire central »</td></tr>
<tr><td></td><td colspan="5"><table>
<tr><th></th><th></th><th></th><th>D</th><th>I</th><th>C</th></tr>
<tr><td rowspan="16">Core Banking System</td><td rowspan="3">Couche</td><td>APP</td><td>4</td><td>4</td><td>4</td></tr>
<tr><td>BDD</td><td>4</td><td>4</td><td>4</td></tr>
<tr><td>OS</td><td>4</td><td>4</td><td>4</td></tr>
<tr><td rowspan="8">Processus métier</td><td>Rapport financier</td><td>4</td><td>4</td><td>4</td></tr>
<tr><td>Gestion des compte clients</td><td>4</td><td>4</td><td>4</td></tr>
<tr><td>Prêt et crédit</td><td>4</td><td>4</td><td>4</td></tr>
<tr><td>Les services de paiement</td><td>4</td><td>4</td><td>4</td></tr>
<tr><td>Provision pour pertes sur créances</td><td>4</td><td>4</td><td>4</td></tr>
<tr><td>Dépôts et retrait</td><td>4</td><td>4</td><td>4</td></tr>
<tr><td>Trésorerie</td><td>4</td><td>4</td><td>4</td></tr>
<tr><td rowspan="5"></td><td>Gestion des clés de sécurité</td><td>4</td><td>4</td><td>4</td></tr>
<tr><td>Développement technologique</td><td>3</td><td>3</td><td>3</td></tr>
<tr><td>Gestion des membres</td><td>3</td><td>3</td><td>4</td></tr>
<tr><td>Gestion de la Continuité des IT</td><td>4</td><td>4</td><td>4</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td>Processus support</td><td>Gestion des Changements</td><td>3</td><td>3</td><td>3</td></tr>
<tr><td></td><td></td><td></td><td></td><td>Gestion des Problèmes</td><td>3</td><td>3</td><td>4</td></tr>
<tr><td></td><td></td><td></td><td></td><td>Gestion des Incidents</td><td>4</td><td>4</td><td>4</td></tr>
<tr><td></td><td></td><td></td><td></td><td>Gestion de la configuration</td><td>2</td><td>2</td><td>4</td></tr>
<tr><td></td><td></td><td></td><td></td><td>Gestion des demandes de service</td><td>4</td><td>4</td><td>3</td></tr>
<tr><td rowspan="5">Service Desk et ITSM</td><td>Utilité de l'application</td><td colspan="5">« Service Desk Application : Cette application est utilisée pour gérer les tickets de support des utilisateurs, suivre les incidents, les demandes de service, et les problèmes techniques »
« facilite la résolution rapide des problèmes et assure un suivi efficace des demandes des utilisateurs. »
« ITSM Application : L'application ITSM (IT Service Management) permet de gérer l'ensemble des services IT selon les meilleures pratiques ITIL »
« il est souvent recommandé d'intégrer les applications Service Desk dans ITSM »</td></tr>
<tr><td>Évaluation de la criticité par couche</td><td colspan="5">« leur non-disponibilité, perte d'intégrité ou non-conformité peuvent perturber les services IT, affecter la productivité des employés, et compromettre la qualité du support utilisateur »
« indirectement affecter les opérations bancaires. »
(Réponses sur tableau)</td></tr>
<tr><td>Processus métier et support</td><td colspan="5">« <u>Service Desk Application :</u>
Processus métier : Gestion des tickets, gestion des incident, exigences réglementaires ainsi que le rapport financier la surveillance des transactions et la conformité réglementaire
Processus support : rapports de performance, gestion des connaissances.
<u>ITSM Application :</u>
Processus métier : Gestion des incidents, des problèmes, des changements, des configurations, et des niveaux de service.
Processus support : tout comme Service Desk Application»</td></tr>
<tr><td>Criticité des processus</td><td colspan="5">« Les processus métier et support des applications Service Desk et ITSM sont critiques pour maintenir une gestion efficace des services IT . »
« des répercussions sur l'ensemble des opérations bancaires »</td></tr>
<tr><td></td><td colspan="5"><table>
<tr><th></th><th></th><th></th><th>D</th><th>I</th><th>C</th></tr>
<tr><td></td><td rowspan="3">Couche</td><td>APP</td><td>4</td><td>3</td><td>3</td></tr>
<tr><td>BDD</td><td>4</td><td>2</td><td>2</td></tr>
<tr><td>OS</td><td>4</td><td>1</td><td>1</td></tr>
<tr><td></td><td rowspan="4">Processus métier</td><td>Rapport financier</td><td>2</td><td>2</td><td>3</td></tr>
<tr><td>Surveillance des transactions</td><td>3</td><td>3</td><td>4</td></tr>
<tr><td>Gestion des tickets</td><td>4</td><td>4</td><td>4</td></tr>
<tr><td>Conformité réglementaire</td><td>3</td><td>3</td><td>4</td></tr>
<tr><td></td><td rowspan="2"></td><td>Gestion des clés de sécurité</td><td>4</td><td>4</td><td>4</td></tr>
<tr><td>Développement technologique</td><td>3</td><td>2</td><td>2</td></tr>
</table></td></tr>
</table>

		Service Desk et ITSM	**Processus support**	Gestion des membres	4	4	4
				Gestion de la Continuité des IT	4	4	4
				Gestion des Changements	4	4	4
				Gestion des Problèmes	4	4	4
				Gestion des Incidents	4	4	4
				Gestion de la configuration	3	3	3
				Gestion des demandes de service	4	4	3

ANNEXE B - TABLEAUX DES RESULTATS DES TESTS DE CONTROLE D'AUDIT

Annexe B01 : Details de date de désactivation de l'accès utilisateur dans l'application CORE_BAKING_SYSTEM_XYZ

Sr. Non	Identifiant/Nom de l'utilisateur	Dernière date de travail	Date de désactivation	Retard de désactivation (nombre de jours de retard)	Commentaires sur KPMG
1	Utilisateur_01	24/03/20XX	26/03/20XX	2	ticket d'id=XXXX1 soulevé le 23/03/20XX
2	Utilisateur_02	18/04/20XX	24/04/20XX	6	ticket d'id=XXXX2 soulevé le 24/04/20XX
3	Utilisateur_03	02/07/20XX	7/4/20XX	2	ticket d'id= XXXX3 soulevé le 04/07/20XX
4	Utilisateur_04	14/07/20XX	16/07/20XX	2	ticket d'id= XXXX4 soulevé le 16/07/20XX
5	Utilisateur_05	16/07/20XX	18/07/20XX	2	ticket d'id= XXXX5 soulevé le 16/07/20XX
6	Utilisateur_06	21/07/20XX	24/07/20XX	3	ticket d'identifiant XXXX6 émis le 20/07/XXXX
7	Utilisateur_07	01/08/20XX	8/2/20XX	1	ticket d'identifiant XXXX7 soulevé le 08/02/20XX
8	Utilisateur_08	8/8/20XX	10/4/20XX	57	ticket d'identifiant XXXX8 soulevé le 03/08/20XX
9	Utilisateur_09	8/11/20XX	13/08/20XX	2	ticket d'identifiant XXXX9 émis le 10/08/20XX
10	Utilisateur_10	14/08/20XX	10/2/20XX	49	ticket d'identifiant XXX10 levé le 16/08/20XX
11	Utilisateur_11	15/08/20XX	17/08/20XX	2	ticket d'identifiant XXX11 raison le 17/08/20XX
12	Utilisateur_12	15/10/20XX	24/10/20XX	9	ticket d'identifiant XXX12 émis le 24/10/20XX

Annexe B02 : Details de configurations de mots de passe pour tous les systèmes concernés au niveau de la couche application et de la couche système d'exploitation

Couche d'application (CORE_BAKING_SYSTEM-APP)			
Sr. Non	**Paramètres**	**Normes de l'industrie**	**Configuration du système**
1	Échec des tentatives de connexion par mot de passe	3	9
2	Historique des mots de passe	24	3

Tableau : Configurations de mots de passe – Couche d'application CORE_BAKING_SYSTEM

Système d'exploitation (CORE_BAKING_SYSTEM -OS)			
Sr. Non	**Paramètres**	**Normes de l'industrie**	**Configuration du système**
1	Historique des mots de passe	24	8
2	Échec des tentatives de connexion par mot de passe	3	5
3	Durée du verrouillage du compte	15 minutes	Pas configuré

Tableau : Configurations de mot de passe – Couche du système d'exploitation CORE_BAKING_SYSTEM

Annexe B03 : Détails des Modifications du Système et État de la Documentation

Sr. Non	Description / Modification liée au fichier système	Demande de changement	Approbation informatique	UAT	Mise en œuvre par
1	Change_Description_01 / System_File_01	Preuve non fournie	Preuve non fournie	Preuve non fournie	Preuve non fournie
2	Change_Description_02 / System_File_02			Preuve non fournie	
3	Change_Description_03 / System_File_03			Preuve non fournie	
4	System_File_04	Preuve non fournie	Preuve non fournie	Preuve non fournie	Preuve non fournie
5	Change_Description_05 / System_File_05			Validation du testing n'as pas été formalisé	
6	Change_Description_06 /System_File_06	Preuve non fournie		Preuve non fournie	
7	Change_Description_07 / System_File_07	Preuve non fournie		Preuve non fournie	
8	Change_Description_08 / System_File_08			Preuve non fournie	
9	Change_Description_09/ System_File_09			Preuve non fournie	
10	Change_Description_10 / System_File_10	Preuve non fournie		Preuve non fournie	

Annexe B04 : Détails des Incidents et Observations sur la Gestion des Incidents

Sr. Non	Numéro d'incident / Description de l'incident	ANS	Date de l'incident soulevée	Date de l'incident clôturée
1	YYYY1 / Incident_Description_01	Moyen	15/06/20XX 16:33	18/06/20XX 08:04
2	YYYY2 / Incident_Description_02	Haut	25/01/20XX 10h18	25/01/20XX 16:18
3	YYYY3 / Incident_Description_03	Haut	31/01/20XX 12:56	02/08/20XX 13:34
4	YYYY4 / Incident_Description_04	Haut	13/02/20XX 09:38	13/02/20XX 16:26
5	YYYY5 / Incident_Description_05	Haut	26/02/20XX 09:52	26/02/20XX 14:14
6	YYYY6 / Incident_Description_06	Haut	16/03/20XX 10h06	16/03/20XX 14:57
7	YYYY7 / Incident_Description_07	Haut	30/04/20XX 16:22	05/11/20XX 15:17
8	YYYY8 / Incident_Description_08	Haut	05/02/20XX 14:55	05/08/20XX 16:16
9	YYYY9 / Incident_Description_09	Haut	05/09/20XX 13:22	10/05/20XX 09:51
10	YYY10 / Incident_Description_10	Haut	29/05/20XX 15:14	30/05/20XX 09:42
11	YYY11 / Incident_Description_11	Haut	01/06/20XX 11:38	06/04/20XX 12:06
12	YYY12 / Incident_Description_12	Haut	26/06/20XX 12:16	02/07/20XX 12:11
13	YYY13 / Incident_Description_13	Haut	17/07/20XX 17:48	25/07/20XX 13:42
14	YYY14 / Incident_Description_14	Haut	08/08/20XX 12:09	14/08/20XX 14:49
15	YYY15 / Incident_Description_15	Haut	16/08/20XX 16:05	17/08/20XX 10:31
16	YYY16 / Incident_Description_16	Haut	31/08/20XX 08:32	31/08/20XX 15:20
17	YYY17 / Incident_Description_17	Haut	09/05/20XX 09:21	10/04/20XX 11:46
18	YYY18 / Incident_Description_18	Haut	14/09/20XX 09:30	14/09/20XX 16:18
19	YYY19 / Incident_Description_19	Haut	26/09/20XX 14:10	10/02/20XX 10:33
20	YYY20 / Incident_Description_20	Haut	10/02/20XX 10:11	10/03/20XX 08:57