

Haute École
« ICHEC – ECAM – ISFSC »



Enseignement supérieur de type long de niveau universitaire

Quel est le degré d'implémentation de l'Intelligence Artificielle (IA) dans la gestion des risques et le contrôle interne des entreprises industrielles ?

Mémoire présenté par :

Alexandre DELA BLANCHERIE

191420

Pour l'obtention du diplôme de :

Master en gestion de l'entreprise

Année académique 2024-2025

Promoteur :

Mathilde FOX

Haute École
« ICHEC – ECAM – ISFSC »



Enseignement supérieur de type long de niveau universitaire

Quel est le degré d'implémentation de l'Intelligence Artificielle (IA) dans la gestion des risques et le contrôle interne des entreprises industrielles ?

Mémoire présenté par :

Alexandre DELA BLANCHERIE

191420

Pour l'obtention du diplôme de :

Master en gestion de l'entreprise

Année académique 2024-2025

Promoteur :

Mathilde FOX

Je souhaite débiter ce travail en remerciant toutes les personnes qui ont contribué, de près ou de loin, à la réalisation de ce mémoire.

Je tiens tout d'abord à remercier ma Promotrice, Madame Mathilde Fox, Enseignante à l'ICHEC en finance, pour ses conseils avisés et son accompagnement tout au long de ce travail.

Je tiens également à remercier tout particulièrement ma maître de stage, Maëlle Valoir, ainsi qu'Émilie Leduc pour leur disponibilité et leurs conseils avisés qui m'ont particulièrement aidé lors de la rédaction de ce travail. Leur expertise a été déterminant dans l'avancement de ce travail.

Je tiens également à remercier mes proches pour leur soutien, leur patience et leur aide à la relecture de ce mémoire.

Je tiens finalement à remercier l'ICHEC et tout le corps professoral pour ces années de formation et les compétences acquises tout au long de mon parcours.

**Déclaration sur l'honneur sur le respect des règles de référencement et sur l'usage des IA
génératives dans le cadre du mémoire ou d'un travail**

« Je soussigné, DELA BLANCHERIE, Alexandre, étudiant en Master Gestion de l'entreprise pour l'année académique 2024-2025, déclare par la présente que le travail ci-joint respecte les règles de référencement des sources reprises dans le règlement des études en signé lors de mon inscription à l'ICHEC (respect de la norme APA concernant le référencement dans le texte, la bibliographie, etc.) ; que ce travail est l'aboutissement d'une démarche entièrement personnelle; qu'il ne contient pas de contenus produits par une intelligence artificielle sans y faire explicitement référence. Par ma signature, je certifie sur l'honneur avoir pris connaissance des documents précités et que le travail présenté est original et exempt de tout emprunt à un tiers non-cité correctement. »

Rixensart, le 19 mai 2025

Je soussigné(e), DELA BLANCHERIE Alexandre – 191420, déclare sur l'honneur les éléments suivants concernant l'utilisation des intelligences artificielles (IA) dans mon mémoire :

Type d'assistance		Case à cocher
Aucune assistance	J'ai rédigé l'intégralité de mon travail sans avoir eu recours à un outil d'IA générative.	
Assistance avant la rédaction	J'ai utilisé l'IA comme un outil (ou moteur) de recherche afin d'explorer une thématique et de repérer des sources et contenus pertinents.	X
Assistance à l'élaboration d'un texte	J'ai créé un contenu que j'ai ensuite soumis à une IA, qui m'a aidé à formuler et à développer mon texte en me fournissant des suggestions.	
	J'ai généré du contenu à l'aide d'une IA, que j'ai ensuite retravaillé et intégré à mon travail.	
	Certains parties ou passages de mon travail/mémoire ont été entièrement été générés par une IA, sans contribution originale de ma part.	
Assistance pour la révision du texte	J'ai utilisé un outil d'IA générative pour corriger l'orthographe, la grammaire et la syntaxe de mon texte.	
	J'ai utilisé l'IA pour reformuler ou réécrire des parties de mon texte.	
Assistance à la traduction	J'ai utilisé l'IA à des fins de traduction pour un texte que je n'ai pas inclus dans mon travail.	
	J'ai également sollicité l'IA pour traduire un texte que j'ai intégré dans mon mémoire.	
Assistance à la réalisation de visuels	J'ai utilisé une IA afin d'élaborer des visuel, graphiques ou images.	
Autres usages		

Je m'engage à respecter ces déclarations et à fournir toute information supplémentaire requise concernant l'utilisation des IA dans mon travail / mémoire, à savoir :

J'ai mis en annexe les questions posées à l'IA et je suis en mesure de restituer les questions posées et les réponses obtenues de l'IA. Je peux également expliquer quel le type d'assistance j'ai utilisé et dans quel but.

Fait à Rixensart, le 19 mai 2025

Signature : Alexandre Dela Blancherie – 191420



Table des matières

PARTIE I – INTRODUCTION.....	1
1. ACTUALITE.....	1
2. METHODOLOGIE GENERALE	3
PARTIE II – ÉTUDE DES CONCEPTS.....	4
1. SECTEUR INDUSTRIEL.....	4
1.1. DEFINITION ET CARACTERISTIQUES	4
1.2. ÉVOLUTION DU SECTEUR	5
1.3. DYNAMIQUE DU SECTEUR	6
1.4. DEFIS ET ENJEUX	7
2. GESTION DES RISQUES	10
2.1. DEFINITIONS	10
2.2.1. Risque	10
2.2.2. Gestion des risques.....	11
2.2. STRATEGIES DE GESTION DES RISQUES	12
2.3. REFERENTIELS	14
2.3.1. COSO ERM (Enterprise Risk Management).....	14
2.3.2. ISO 31000.....	16
2.4. LIMITES DE LA GESTION DE RISQUES.....	16
2.4.1. Limites du processus de définition des risques	16
2.4.2. Les influences sociales	17
2.4.3. La cartographie des risques	17
2.4.4. Les heuristiques et biais cognitifs	18
3. CONTROLE INTERNE.....	19
3.1. DEFINITION	19
3.2. LIGNES DE DEFENSE.....	21
3.3. REFERENTIEL – COSO.....	22
3.3.1. Objectifs de contrôle	23
3.3.2. Niveaux de responsabilités	23
3.3.3. Éléments de contrôle.....	23
3.4. LIMITES ET DEFICIENCES DU CONTROLE INTERNE	25
3.4.1. Limites liées au coût	25
3.4.2. Limites liées au jugement	25
3.4.3. Limites liées aux défaillances.....	26
3.4.4. Limites liées à la dérogation de gestion (Management Override)	26
3.4.5. Collusion	26
4. INTELLIGENCE ARTIFICIELLE	27
4.1. DEFINITION	27
4.2. HISTOIRE	28
4.3. TYPES D’INTELLIGENCES ARTIFICIELLES	30
4.4. LES MODELES D’INTELLIGENCE ARTIFICIELLE : LE MACHINE LEARNING	31
4.4.1. Machine Learning (ML).....	31
4.4.2. Les paradigmes d’apprentissage	31
4.4.3. Réseaux de neurones (Neural Networks)	32
4.4.4. Deep Learning (DL)	33
4.4.5. Natural Language Processing (NLP)	34

4.5. APPLICATIONS DE L'IA	35
4.6. LIMITES, BIAIS ET ETHIQUE.....	36

PARTIE III – QUESTION DE RECHERCHE38

1. QUESTION DE RECHERCHE	38
2. HYPOTHESES	39
2.1. HYPOTHESE 1	39
2.2. HYPOTHESE 2	39
2.3. HYPOTHESE 3	39

PARTIE IV – REVUE SPECIFIQUE DE LA LITTERATURE40

1. OBJECTIFS DE L'ETUDE	40
2. TECHNOLOGY ACCEPTANCE MODEL (TAM)	41
3. FACTEURS INFLUENÇANT L'ADOPTION DE L'IA.....	43
3.1. FACTEURS ORGANISATIONNELS ET HUMAINS	43
3.2. FACTEURS FINANCIERS	44
3.3. FACTEURS LEGAUX.....	45
3.4. FACTEURS ETHIQUES	47
4. L'INTELLIGENCE ARTIFICIELLE DANS LE CONTROLE INTERNE ET LA GESTION DES RISQUES	49
4.1. APPLICATIONS ACTUELLES DE L'IA DANS LE CONTROLE INTERNE.....	49
4.2. APPLICATIONS ACTUELLES DANS LA GESTION DES RISQUES	50
4.3. LIMITES DE L'INTELLIGENCE ARTIFICIELLE DANS LE CONTROLE INTERNE ET LA GESTION DES RISQUES	51
4.4. ÉTAT ACTUEL DE L'ADOPTION DE L'INTELLIGENCE ARTIFICIELLE DANS LE SECTEUR INDUSTRIEL	53
4.4.1. Adoption globale de l'Intelligence Artificielle dans les entreprises	53
4.4.2. Adoption de l'Intelligence Artificielle dans les entreprises industrielles	56
4.4.3. Adoption de l'Intelligence Artificielle dans le contrôle interne des entreprises industrielles.....	57
4.4.4. Adoption de l'Intelligence Artificielle dans la gestion des risques des entreprises industrielles.....	59
4.5. COMPARAISON AVEC D'AUTRES SECTEURS	60
5. CONCLUSION	62

PARTIE V – ÉTUDE EMPIRIQUE64

1. OBJECTIFS	64
2. ÉTUDE QUANTITATIVE	65
2.1. CONSTRUCTION DE L'OUTIL DE RECOLTE DE DONNEES.....	65
2.1.1. Classification des entreprises par taille	65
2.1.2. Détermination du degré d'implémentation de l'Intelligence Artificielle	66
2.1.3. Degré d'implémentation de l'IA dans la gestion des risques	66
2.1.4. Degré d'implémentation dans le contrôle interne	66
2.1.5. Cible	67
2.2. ANALYSE DES DONNEES	68
3. ÉTUDE QUALITATIVE	70
3.1. ÉLABORATION DU GUIDE D'ENTRETIEN	70
3.2. RESULTATS DE L'ETUDE QUALITATIVE	71
3.2.1. Degré d'implémentation de l'Intelligence Artificielle.....	71

3.2.2. Applications de l'Intelligence Artificielle	71
3.2.3. Risques de l'Intelligence Artificielle.....	72
3.2.4. Limites de l'Intelligence Artificielle.....	73
4. CONCLUSION	74

PARTIE VI – DISCUSSION76

1. APPLICATIONS DE L'INTELLIGENCE ARTIFICIELLE	76
2. RISQUES DE L'INTELLIGENCE ARTIFICIELLE.....	77
3. LIMITES DE L'INTELLIGENCE ARTIFICIELLE	78
4. HYPOTHESES	79
4.1. HYPOTHESE 1	79
4.2. HYPOTHESE 2	80
4.3. HYPOTHESE 3	80

PARTIE VII – LIMITES DE L'ETUDE81

PARTIE VIII – PISTES POUR DES RECHERCHES FUTURES82

PARTIE IX – CONCLUSION GENERALE83

BIBLIOGRAPHIE86

Liste des figures

<i>Figure 1 : Structure du secteur industriel</i>	<i>4</i>
<i>Figure 2 : Historique des émissions de gaz à effet de serre</i>	<i>8</i>
<i>Figure 3 : Cycle de gestion des risques</i>	<i>11</i>
<i>Figure 4 : Exemple de cartographie des risques</i>	<i>12</i>
<i>Figure 5 : L'échelle sévérité/fréquence</i>	<i>13</i>
<i>Figure 6 : Les huit composantes de la gestion des risques</i>	<i>14</i>
<i>Figure 7 : Modèles des trois lignes de défense</i>	<i>22</i>
<i>Figure 8 : COSO I</i>	<i>22</i>
<i>Figure 9 : Test de Turing</i>	<i>28</i>
<i>Figure 10 : Les modèles d'Intelligence Artificielle</i>	<i>31</i>
<i>Figure 11 : Illustration d'un réseau de neurones simple et d'un réseau de neurones profond</i>	<i>33</i>
<i>Figure 12 : Tâches du Natural Language Processing</i>	<i>34</i>
<i>Figure 13 : Modèle d'acceptation de la technologie</i>	<i>41</i>
<i>Figure 14 : Maturité de l'IA en fonction de la taille</i>	<i>54</i>
<i>Figure 15 : État des lieux de l'implémentation de l'IA dans les entreprises</i>	<i>54</i>
<i>Figure 16 : Niveau d'intérêt de l'IA générative</i>	<i>55</i>
<i>Figure 17 : Where does biopharma stand on the AI maturity curve ?</i>	<i>56</i>
<i>Figure 18 : Niveau de maturité du cadre de contrôle interne en matière de digitalisation</i>	<i>58</i>
<i>Figure 19 : Cas d'usage de l'IA en gestion des risques</i>	<i>59</i>
<i>Figure 20 : Répartition de la maturité de l'IA par secteur</i>	<i>60</i>
<i>Figure 21 : Utilisation d'outils IA par secteur</i>	<i>61</i>
<i>Figure 22 : Seuils pour les petites et grandes sociétés</i>	<i>65</i>
<i>Figure 23 : Seuils pour les microsociétés</i>	<i>65</i>
<i>Figure 24 : Échelle d'évaluation de l'IA dans le contrôle interne et la gestion des risques</i>	<i>66</i>
<i>Figure 25 : Poids du niveau d'implémentation de l'IA</i>	<i>67</i>

Partie I – Introduction

Le monde dans lequel nous vivons évolue avec une rapidité extrême, entraînant au passage de nombreuses conséquences pour les entreprises mais également pour les individus. Les apports des nouvelles technologies, notamment l'intelligence artificielle, exercent une pression considérable sur les systèmes actuels car elles imposent aux entreprises de maîtriser ces nouvelles technologies afin de rester compétitives. Des technologies telles que l'intelligence artificielle ont des applications qui sont de plus en plus nombreuses, y compris dans des domaines que l'on pensait peu automatisables, en ce compris la gestion des risques des entreprises, mais également les contrôles qu'elles mettent en place.

1. Actualité

Une mauvaise gestion des risques auxquels est confrontée une entreprise peut avoir des conséquences irréversibles, peu importe sa puissance ou sa taille. L'histoire nous l'a déjà démontré ; aucune entreprise n'est à l'abri d'une faillite si elle ne prend pas suffisamment en considération l'évolution de son environnement et les risques qu'il engendre.

Le 15 septembre 2008 marque la chute d'une des plus grandes institutions financières des États-Unis, celle de Lehman Brothers. Elle demeure aujourd'hui encore la plus grosse faillite de l'histoire avec une perte estimée à plus de 600 milliards de Dollars et elle est la preuve que la taille et la puissance d'une entreprise sur son marché n'ont aucun pouvoir face à une prise de risques incontrôlée et un manque de supervision de certaines opérations sensibles. Mais que s'est-il réellement passé pour que cette banque devienne "un colosse aux pieds d'argile" et ne finisse par s'effondrer et entraîner dans sa chute les investissements de millions de personnes (Goetz & Grandin, s.d.)?

Remettons cette faillite dans son contexte. Nous sommes en plein coeur de la crise des "Subprimes", une crise financière causée par un excès d'endettement des particuliers aux États-Unis, et qui se propagera rapidement au reste du monde. Les subprimes sont en fait des prêts immobiliers accordés à des Américains avec une mauvaise solvabilité à partir des années 2000. Ces prêts leur sont accordés dans le but de relancer le marché immobilier aux États-Unis en rendant les prêts plus accessibles. Ces prêts à faible coût vont entraîner une hausse des prix de l'immobilier américain et donc une demande de prêts de plus en plus grands. Ceci créera une bulle spéculative qui engendrera à son tour la crise financière de 2008 (La finance pour tous, 2024).

Tous ces prêts à haut risques accordés étaient rassemblés et transformés en titres que les banques s'échangeaient ensuite. C'est ce que l'on appelle la titrisation. Lehman Brothers a même créé une filiale dédiée à cette activité, BNC Mortgage. Cela finit par rapporter plus de 4 milliards de dollars américain à Lehman Brothers mais l'erreur qui a été commise par Richard Fuld, CEO de Lehman Brothers lors de la crise, c'est d'avoir un ratio d'endettement-liquidités

bien plus grand que la plupart des autres banques. Là où la plupart des banques avaient un ratio d'un dollar de capital pour 25 dollars empruntés, Lehman Brothers avait un ratio d'un pour 30. Nous pouvons donc relever l'une des premières raisons qui ont conduit Lehman Brothers à mettre la clé sous la porte, qui n'est autre qu'une mauvaise gestion de ses risques (Goetz & Grandin, s.d.).

Un autre élément important à prendre en considération dans l'affaire Lehman Brothers est le camouflage de ses dettes avant la publication des bilans via des pratiques comptables consistant à revendre des titres contre du cash dans le but de garder la confiance de ses investisseurs, de ses clients et de ses employés. C'est ici donc la preuve que Lehman Brothers savait qu'elle était en mauvaise posture et qu'elle ne voulait pas éveiller des soupçons quant à sa mauvaise santé financière. Cela démontre donc qu'il y avait un manque accru de contrôle des procédures au sein de la banque (Goetz & Grandin, s.d.).

Bien entendu, ceci n'est pas le seul cas où une mauvaise gestion des risques et un contrôle des procédures négligé ont eu des conséquences désastreuses. Ainsi, en 2008, Jérôme Kerviel, un trader pour la Société Générale, est accusé d'avoir causé une perte de pas moins de 4,9 milliards d'euros à la Société Générale à la suite de transactions non-autorisées (Dumas, s.d.). Dans les faits, il aurait pris des positions financières à hauteur de 50 milliards d'euros, ce qui représentait plus que la totalité des fonds de la banque à ce moment, entraînant inévitablement un risque conséquent de faillite pour la Société Générale en cas de chute du marché. Ces positions dépassaient évidemment largement les seuils qui lui étaient autorisés de placer et Mr. Kerviel était bien conscient de cela (Société Générale, 2016). C'est la raison pour laquelle il a dissimulé ces transactions par des opérations fictives, afin de donner l'illusion qu'il maîtrisait les risques en contournant au passage le contrôle interne mis en place par la banque (Dumas, s.d.).

La perte de 4,9 milliards d'euros est en réalité une perte nette. La perte totale, après la revente de ses positions par la Société Générale, était estimée à 6,3 milliards d'euros, compensée par des gains que Jérôme Kerviel avait réalisés pour une valeur totale de 1,4 milliard d'euros (Société Générale, 2016).

C'est ici encore la preuve que cette perte colossale est la conséquence d'une faille dans les contrôles des procédures de la Société Générale et plus précisément la supervision de ses traders et leurs prises de positions et manipulations comptables. Il s'agit également d'une prise de risque inconsidérée de la part de Jérôme Kerviel, tant pour lui-même que pour la société pour laquelle il travaillait. Dans ce cas-ci, la Société Générale n'a pas fait faillite mais a tout de même frôlé une catastrophe, tant financière que médiatique.

Ces deux études de cas démontrent clairement l'importance de la gestion des risques et de la mise en place d'un contrôle rigoureux des procédures au sein d'une entreprise, et dans ces cas-ci dans des banques. Ce sont des éléments qui n'étaient visiblement pas parfaitement maîtrisés, rendant l'entreprise vulnérable en cas de changement de tendances du marché ou rendant une faille exploitable par un employé sans que l'entreprise ne puisse s'en rendre compte avant qu'il ne soit trop tard.

2. Méthodologie générale

Ce mémoire a pour objectif de démontrer que les nouvelles technologies, et plus particulièrement l'intelligence artificielle, peuvent apporter un soutien aux entreprises afin d'améliorer la gestion de leurs risques et le contrôle de leurs procédures. Ce travail se focalisera majoritairement sur le secteur industriel, un secteur essentiel au fonctionnement de notre économie qui a connu de nombreux bouleversements au cours des derniers siècles.

Nous commencerons ce travail par une étude précise du secteur industriel, de la gestion des risques, du contrôle interne, mais également de l'intelligence artificielle. Cette étude passera par une définition complète du concept en question, mais également la description de ses composantes, ses limites, ainsi que, le cas échéant, de son histoire et des défis liés au concept. Cette étude permettra une compréhension approfondie des concepts utilisés dans la suite de ce travail. Sur base de l'introduction et des concepts, nous élaborerons également une question de recherche ainsi que des hypothèses, qui serviront de guide pour la suite.

Une fois la question de recherche définie et les hypothèses établies, nous continuerons les investigations par une revue de la littérature. Celle-ci permettra d'apporter des bases théoriques solides pour répondre à la question de recherche. Nous étudierons premièrement les facteurs théoriques pouvant expliquer les résultats que nous obtiendrons à l'issue de cette étude. Nous développerons également les applications de l'intelligence artificielle pour améliorer la gestion des risques d'une entreprise, mais également les contrôles qu'elle met en place. Finalement, nous adopterons une stratégie en entonnoir afin de voir à quel point l'intelligence artificielle est déjà utilisée dans les entreprises de manière générale. Par la suite, nous rétrécirons ce spectre pour se focaliser uniquement sur les entreprises du secteur industriel. Finalement l'objectif sera d'évaluer à quel point l'intelligence artificielle est utilisée par les entreprises industrielles pour gérer leurs risques et effectuer leurs contrôles.

Afin de nuancer les résultats obtenus lors de la revue de la littérature, nous effectuerons ensuite une étude empirique basée sur deux études distinctes. D'une part, nous procéderons à une étude quantitative afin de mesurer le degré d'adoption de l'intelligence artificielle dans la gestion des risques et les contrôles des entreprises industrielles belges. D'autre part, nous ferons une étude qualitative en procédant à des entretiens avec des expertes en intelligence artificielle et en gestion des risques et contrôles.

Cette approche théorique et pratique permettra d'apporter une réponse nuancée à la question de recherche formulée, mais également de confirmer ou non les hypothèses énoncées. Ce travail se basera essentiellement sur des sources scientifiques spécialisées, ainsi que sur des rapports publiés par des entreprises expertes. De cette manière, nous obtiendrons une approche riche et pertinente pour répondre à la question de recherche de manière la plus objective possible.

Partie II – Étude des concepts

1. Secteur industriel

1.1. Définition et caractéristiques

Le secteur industriel, ou secteur secondaire, est un secteur essentiel de notre économie car il est responsable de la production de biens nécessaires à la production d'autres biens ou la réalisation d'autres activités. Comme représenté sur le schéma ci-dessous, le secteur industriel comprend trois catégories distinctes : l'industrie manufacturière, l'industrie agro-alimentaire et l'industrie de l'énergie. L'industrie manufacturière est elle-même subdivisée en 3 ensembles : l'industrie produisant des biens intermédiaires (métallurgie, chimie, papier, plastiques, verre), l'industrie des biens d'équipements d'entreprises (machines, matériel électronique, construction navale et aéronautique) et l'industrie des biens de consommation (pharmacie, textile, ameublement, parachimie, ...) (Capul & Garnier, 2017).

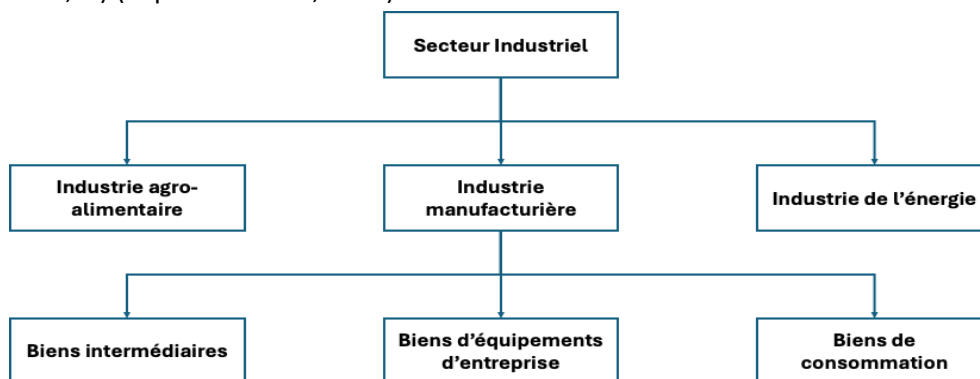


Figure 1 : Structure du secteur industriel (Capul & Garnier, 2017)

D'autres distinctions peuvent être faites entre les différentes industries telles que les industries lourdes (telles que la sidérurgie, la chimie) en opposition aux industries légères ou encore les biens de production en opposition aux biens de consommation (Capul & Garnier, 2017).

L'Institut National de la Statistique et des Études Économiques (INSEE) définit le secteur industriel comme étant des « activités économiques qui combinent des facteurs de production (installations, approvisionnements, travail, savoir) pour produire des biens matériels destinés au marché » (Institut National de la Statistique et des Études Économiques (INSEE), 2021).

Il est important de noter le fait que, en Europe, l'industrie représente plus de 23% du PIB en moyenne. Au Luxembourg par exemple, l'industrie ne représente que 10% du PIB en 2022 là où en Norvège, elle représente 49% du PIB en 2022 (Gaudiaut, 2024).

Nous pouvons donc en déduire que le secteur industriel ou secteur secondaire a pour objectif de transformer des matières premières issues du secteur primaire ou des produits semi-finis, afin de les revendre à d'autres entreprises ou particuliers en utilisant pour ce faire des facteurs de production. C'est un secteur-clé de notre économie car de nombreuses autres activités en dépendent.

1.2. Évolution du secteur

L'histoire du secteur industriel est jalonnée de grandes évolutions que nous appelons révolutions industrielles. Celles-ci ont profondément métamorphosé les modes de production, la manière dont le travail est organisé et la société en général. Depuis le 18^e siècle, le monde a connu quatre grandes révolutions industrielles.

La première révolution industrielle date de la fin des années 1760 en Angleterre. Elle s'est ensuite propagée dans d'autres pays tels que la France, les États-Unis, le Canada et l'Allemagne. Cette révolution est marquée par l'arrivée du moteur à vapeur, développé par James Watt. Celui-ci permettra la mécanisation du travail et augmentera considérablement l'efficacité de la production. Cette invention est la source de la modification des modes de production et du travail dans le monde (Brenet, 2024).

L'automatisation des métiers à tisser, également appelés navettes volantes, ont révolutionné l'industrie du textile. En 1815, la première machine à vapeur à usage industriel est créée, entraînant une croissance exponentielle de la population au Royaume-Uni. Une transition se fait alors d'une économie basée sur l'agriculture vers une économie basée sur le charbon. Cette révolution a entraîné des changements économiques et sociaux majeurs et a servi de base pour les révolutions industrielles suivantes (Brenet, 2024).

La seconde révolution industrielle, débutant dans les années 1870, est marquée par l'introduction de l'électricité, du pétrole, de la chimie et de la mécanique, bouleversant encore davantage la manière dont le travail était organisé. L'invention du moteur à explosion changea radicalement les moyens de transport et la production d'énergie. L'industrie chimique a également fait des progrès significatifs, permettant la création de nouveaux matériaux et de produits chimiques. Cette période a également vu émerger des nouveaux moyens de communication tels que le téléphone et la radio, métamorphosant la manière dont les informations étaient transmises (Brenet, 2024).

La seconde révolution industrielle est également marquée par la consolidation de l'économie autour de grandes entreprises. Ces entreprises ont réussi à étendre leur portée au-delà de leurs frontières, marquant le début de la mondialisation. La seconde révolution industrielle prend fin avec le début de la Première Guerre mondiale (Brenet, 2024).

La troisième révolution industrielle, autrement appelée révolution scientifique et technique, est marquée par l'arrivée des technologies électroniques et informatiques dans les années 1970. L'arrivée du microprocesseur transformera radicalement l'industrie et la société. Cette révolution industrielle voit apparaître des matériaux révolutionnaires tels que les résines, les silicones ou encore les céramiques, essentiels au développement de nouvelles technologies (Brenet, 2024).

Les années 1990, connaissent une croissance fulgurante d'Internet et autres technologies de l'information, révolutionnant encore de façon durable la manière dont les individus communiquent entre eux et dont ils ont accès à l'information (Brenet, 2024).

Nous entendons parler pour la première fois de la quatrième révolution industrielle ou encore de l'industrie 4.0 en 2011 en Allemagne. C'est lors d'un salon sur la technologie industrielle prenant place à Hanovre en Allemagne que celle-ci présente l'industrie 4.0 comme un projet ambitieux concernant leur stratégie industrielle. Leur objectif était alors de moderniser leur industrie à l'aide de nouvelles technologies telles que l'intelligence artificielle, la robotique et Internet des objets (Internet of Things, IoT) (Brenet, 2024).

L'industrie 4.0 est synonyme d'intégration des nouvelles technologies dans l'ensemble des processus industriels, permise par l'utilisation de capteurs intelligents, d'outils d'analyse de données, de la connectivité entre les machines mais également de l'automatisation intelligente des tâches. L'objectif final est d'accroître l'efficacité de la production, en la rendant plus flexible en étant capable de s'ajuster de manière autonome au marché (Brenet, 2024).

Nous pouvons donc constater que le secteur a subi de nombreuses transformations depuis le 18^e siècle et nous venons de rentrer dans une nouvelle ère, celle d'une industrie technologique. Il sera primordial, tant pour les nouvelles entreprises que les entreprises existantes, de s'intéresser et d'investir dans ces nouvelles technologies dans le but de rester compétitives sur un marché évoluant de plus en plus rapidement.

1.3. Dynamique du secteur

La santé du secteur industriel à travers le monde est loin d'être uniforme, chaque région du monde évolue à un rythme différent. L'Europe doit faire face à une variation importante de la demande. En effet, des facteurs tels que des taux d'intérêts élevés qui freinent les investissements ou encore les stocks excédentaires dus à des commandes excessives lors des années précédentes font que les industries ont plus de mal à prévoir leur demande (Bokeria et al., 2025).

En Belgique, la situation se dégrade. En effet, entre 2022 et 2023, la valeur totale de la production industrielle a diminué de 9%, passant de 216 milliards d'euros à 196 milliards d'euros et il existe de nombreux cas pouvant attester de la situation (Statbel, 2025).

Le 28 février 2025 marque la date de fermeture définitive de l'usine Audi Brussels, supprimant pas moins de 3.000 emplois. Cette usine active depuis 1949 était l'une des dernières usines automobiles encore actives en Belgique. Sa fermeture reflète les difficultés de l'industrie belge.

Il y a trois raisons principales qui font que l'usine bruxelloise a dû fermer. La première raison est la baisse de la demande du modèle Q8 e-tron, un véhicule produit dans l'usine qui a énormément souffert de la concurrence. Une autre raison est liée aux coûts d'exploitation élevés en comparaison avec d'autres pays en Europe, rendant la production de ce véhicule moins attractive que dans un autre pays. Finalement, aucun acheteur n'a été trouvé pour l'usine bien que de nombreuses recherches aient été effectuées et que certains groupes automobiles chinois s'y soient intéressés (Stroobants, 2025).

Cette fermeture fût un électrochoc pour beaucoup de personnes en Belgique et plusieurs experts soulignent le fait que l'attractivité industrielle belge est assez faible en raison de sa fiscalité et de son coût de l'énergie. Sa fermeture est perçue comme un symbole de la désindustrialisation de la Belgique (Stroobants, 2025).

Aux États-Unis, la tendance est différente qu'en Europe. Ils investissent massivement dans la recherche et le développement et notamment dans les technologies de pointe (source xxx). Il faut d'ailleurs mentionner le fait que les investissements industriels européens sont plus importants aux États-Unis qu'en Europe. En 2024, on estime que 37% des investissements industriels étaient destinés aux Etats-Unis contre 33% pour l'Union Européenne et le Royaume-Uni (Djossou, 2024).

En Asie, nous pouvons constater un changement de direction dans le but de poursuivre sa croissance économique. La croissance industrielle y ralentit car les pays asiatiques voient un grand potentiel dans les services modernes tels que les fintechs, les technologies de l'information etc. (Baba et al., 2024).

1.4. Défis et enjeux

Le secteur industriel connaît depuis de nombreuses années des transformations importantes qui ont changé pour toujours le fonctionnement des industries dans le monde entier. Ces transformations ont été extrêmement bénéfiques pour les industries ainsi que pour les consommateurs mais le secteur est aujourd'hui, plus que jamais, confronté à des défis et des enjeux de taille.

La durabilité préoccupe davantage la population qu'auparavant et nous faisons face à une prise de conscience générale que des actions doivent être prises sans plus tarder si nous voulons nous assurer un futur viable. Comme le démontre le graphique ci-dessous, cette prise de conscience est visible depuis le début des années 2000. En effet, depuis 1990 (année de référence), les émissions de gaz à effet de serre ont diminué d'environ 30%, grâce notamment à de nouvelles normes mises en place dans le but de réduire ces émissions. (Climat.be, 2025).

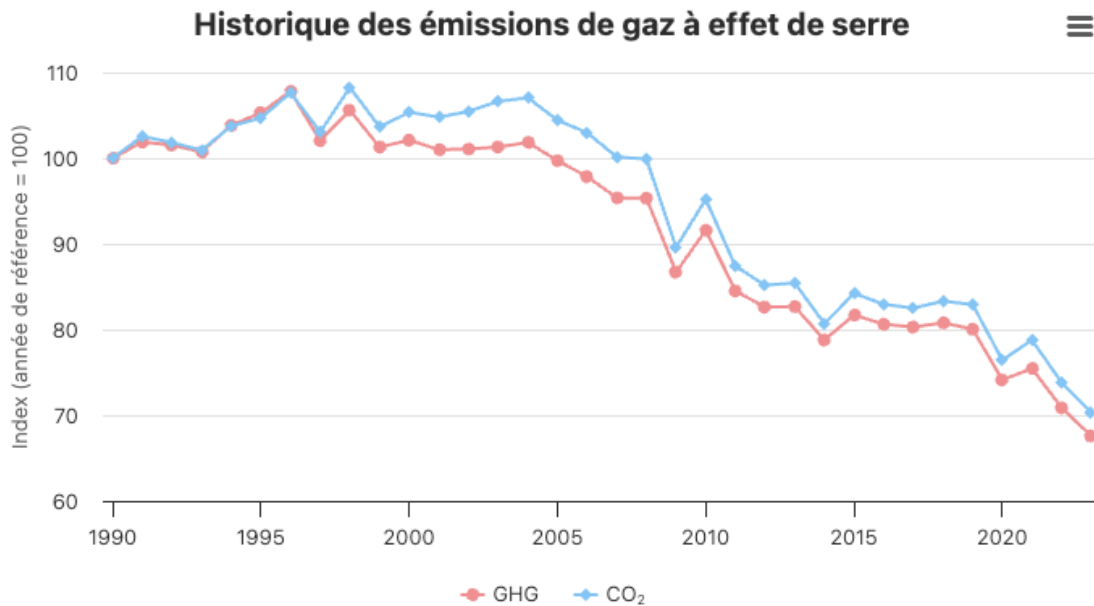


Figure 2 : Historique des émissions de gaz à effet de serre

Source : Climat.be. (2025). *Historique des gaz à effet de serre*. Consulté le 14 avril 2025 à l'adresse <https://climat.be/en-belgique/climat-et-emissions/emissions-des-gaz-a-effet-de-serre/historique>

Il faut savoir que le secteur industriel est responsable d'environ 21% des émissions mondiales de gaz à effet de serre. Celles-ci proviennent principalement de la production d'acier, de ciment et autres produits chimiques mais également des énergies fossiles nécessaires à la production de certains biens (D-Carbonize, 2025).

L'adoption de nouvelles technologies dans le but de gagner en efficacité, tant d'un point de vue énergétique que d'un point de vue production, permettrait de réduire drastiquement les émissions de gaz à effet de serre.

L'ESG (Environnement, Social, Gouvernance), connaît également une ascension exponentielle depuis quelques années et constitue un cadre utilisé afin de mesurer les performances non financières d'une entreprise. C'est un moyen pour les parties prenantes de connaître le positionnement d'une entreprise concernant ces 3 aspects et les investisseurs considèrent de plus en plus les scores ESG comme des indicateurs primordiaux, reflétant la solidité et la durabilité d'une entité (PlanA, s.d.). Les entreprises industrielles ont donc un grand intérêt à travailler sur l'amélioration de leurs scores ESG dans le but de rester compétitives et attractives sur le marché.

L'aspect digital peut être bénéfique pour le secteur industriel mais il apporte également son lot de difficultés. Des robots sont capables de réaliser de nombreuses tâches répétitives mais il est parfois difficile de combiner des facteurs de production humains et des robots. L'adoption massive de l'intelligence artificielle va bouleverser avec certitude l'ensemble du secteur, si ce n'est déjà le cas. Néanmoins, comme nous le verrons dans un chapitre suivant (cf. Chapitre 4), le développement d'une intelligence artificielle est extrêmement complexe et coûteux, tant en termes de temps que sur le plan financier. La question de la sécurité des données peut également poser des problèmes, car avec la croissance des objets connectés, les possibilités de fuites

d'informations sensibles augmentent également, représentant un risque considérable pour les entreprises (Azumata, 2024).

Du point de vue des ressources humaines, le secteur industriel doit aussi faire face à un défi de taille, à savoir une pénurie de la main d'œuvre qualifiée et un vieillissement de la population active. Une étude menée en France a démontré que pour plus d'un décideur sur deux, le secteur industriel n'est pas assez attractif et ils estiment que les salaires devraient être revus à la hausse, que les conditions de travail devraient être améliorées ou encore que des formations spécifiques devraient être mises en place pour augmenter l'attractivité du secteur. Il faut en somme parvenir à changer la perception que le monde a du secteur en lui faisant comprendre que l'industrie a drastiquement changé avec l'arrivée des nouvelles technologies et qu'il est désormais tourné vers l'innovation (Bonnefous, 2024).

Il faut également mentionner le fait que l'arrivée des nouvelles technologies dans le secteur industriel créera inévitablement des nouveaux emplois, spécifique à la gestion et la maintenance de ces nouvelles technologies, mais entraînera malencontreusement la disparition de certains postes, voués à être remplacés par des robots ou autres systèmes. On estime que, d'ici 2030, 170 millions de nouveaux emplois seront créés, supprimant au passage 92 millions de postes (Forum Économique Mondial, s.d.).

2. Gestion des risques

Nous avons pu constater dans l'analyse de l'actualité développée au début de ce travail que l'environnement dans lequel évoluent les entreprises est un environnement incertain et qu'une bonne gestion de risques est primordiale à leur survie. Une gestion de risques négligée, même pour les entreprises que l'on pourrait croire invincibles, serait dévastatrice, comme nous l'a démontré la faillite de Lehman Brothers en 2008, par exemple.

2.1. Définitions

2.2.1. *Risque*

Avant de définir ce que nous entendons par gestion des risques, il est important de revenir sur la notion de « Risque ». En 2004, le COSO (Committee of Sponsoring Organizations of the Treadway Commission) a défini un risque de la manière suivante : « Constituent des risques, les événements probables ayant un impact négatif et pouvant freiner la création de valeur ou détruire la valeur existante. » (Cordel, 2019).

Le risque peut être calculé en multipliant sa probabilité d'occurrence et son impact :

$$\textbf{Risque} = \textbf{Probabilité} \times \textbf{Impact}$$

Il existe également de nombreux types de risques pouvant être regroupés dans diverses catégories, certaines classifications étant plus pertinentes que d'autres. Nous reprendrons ici uniquement les catégories qui se veulent être les plus pertinentes dans le cadre de ce travail (Cordel, 2019).

Nous pouvons tout d'abord faire la distinction entre les **risques purs** et les **risques spéculatifs**. Un risque pur est un risque dont la conséquence ne peut être que négative tel que par exemple un incendie. Au contraire, un risque spéculatif est un risque dont l'occurrence peut avoir des impacts négatifs comme positifs, tels que la variation d'un taux d'intérêt par exemple (Cordel, 2019).

Nous pouvons également faire la distinction entre un **risque interne** et un **risque externe**. Les risques externes sont des risques qui ne résultent pas d'une action faite par l'entreprise. En d'autres termes ce sont des risques exogènes à l'entreprise. Un risque interne est au contraire endogène à l'entreprise et par conséquent, ce sont des risques que l'entreprise peut maîtriser (Cordel, 2019).

Une distinction peut également être faite entre les **risques économiques** et les **risques financiers**. Les risques financiers regroupent les risques de liquidité, les risques de crédit, et le risque de taux et sont dans la majeure partie des cas exogènes à l'entreprise. Un risque économique se réfère plutôt aux conditions macroéconomiques telles que le taux de chômage, la croissance, l'inflation, etc. (Cordel, 2019).

Finalement, il peut être intéressant de distinguer les **risques inhérents** et les **risques résiduels**. Un risque inhérent ou risque brut est la qualification d'un risque avant que toute mesure ne soit prise par l'entreprise pour le limiter. Au contraire, un risque résiduel ou risque net représente le niveau de risque supporté par l'entreprise après avoir considéré les stratégies de gestion (Cordel, 2019).

$$\textbf{Risque net} = \textbf{Risque brut} - \textbf{Stratégies de gestion}$$

Un univers de risques représente l'ensemble des risques auxquels une entreprise est exposée (Cordel, 2019).

2.2.2. Gestion des risques

La gestion de risques est, d'après le COSO (Committee of Sponsoring Organizations of the Treadway Commission), « un processus mis en œuvre par le conseil d'administration, la direction générale, le management et l'ensemble des collaborateurs de l'organisation. Il est pris en compte dans l'élaboration de la stratégie ainsi que dans toutes les activités de l'organisation. Il est conçu pour identifier les événements potentiels susceptibles d'affecter l'organisation et pour gérer les risques dans les limites de son appétence pour le risque. Il vise à fournir une assurance raisonnable quant à l'atteinte des objectifs de l'organisation. » (Cordel, 2019).

Le processus de gestion des risques est un cycle ayant pour objectif de traiter tous les risques de manière cohérente. Comme représenté sur la figure ci-dessous, le processus de gestion des risques est un cycle comportant 4 activités : l'identification, l'évaluation, la réponse au risque et la surveillance (Sholtissen, 2024).

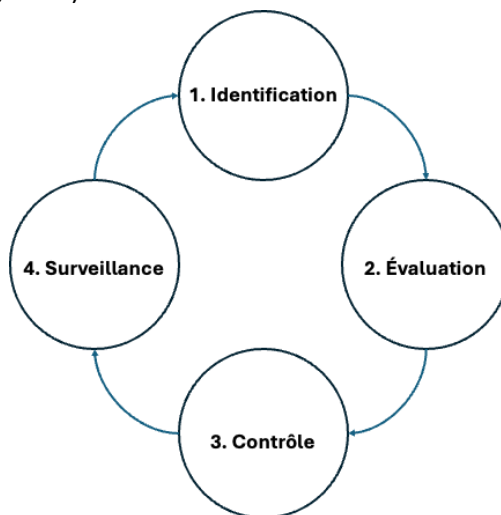


Figure 3 : Cycle de gestion des risques (Sholtissen, 2024).

L'identification consiste tout simplement à établir la liste des risques auxquels l'entreprise est confrontée durant l'exercice de son activité. L'évaluation des risques consiste à évaluer la sévérité du risque s'il devait se produire ainsi que la probabilité que celui-ci ne se réalise. Le contrôle est l'étape où nous définissons les stratégies pour limiter l'impact de ce risque.

Finalement, la surveillance consiste à évaluer si la situation a changé et si de nouveaux risques sont apparus. La gestion des risques est donc un cycle car rien n’est figé. L’environnement d’une entreprise évolue constamment et de nouveaux risques peuvent apparaître et c’est la raison pour laquelle il est important de répéter ce cycle (Sholtissen, 2024). Ces étapes seront développées de manière plus détaillée dans la partie consacrée au référentiel COSO II.

Lors de l’évaluation des risques, il est possible d’établir une cartographie des risques en leur associant un impact et une probabilité que ceux-ci se produisent. Cette cartographie permet d’identifier de manière visuelle les risques les plus importants et d’identifier les stratégies les plus appropriées pour gérer ces risques (Sholtissen, 2024).

Le tableau suivant est un exemple de cartographie des risques reprenant en ordonnées la probabilité que le risque se réalise et en abscisses l’impact du risque s’il se réalise.

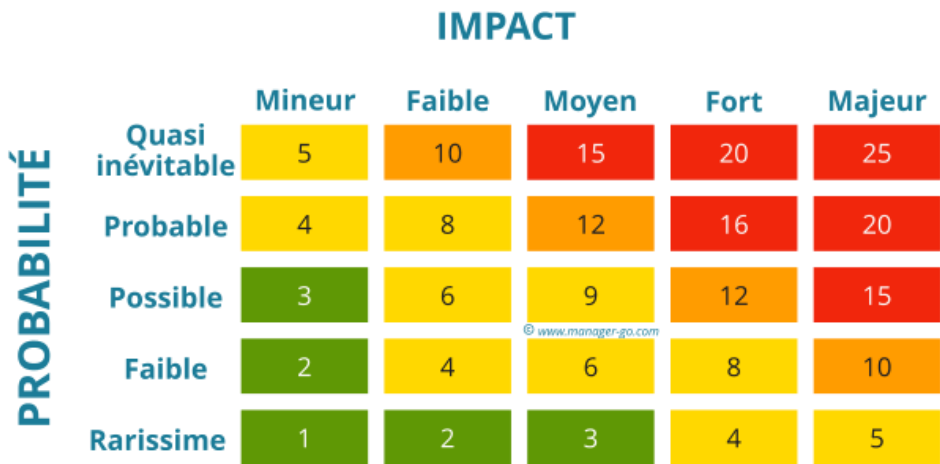


Figure 4: Exemple de cartographie des risques
 Source : Guigon, C. (2024). Cartographie des risques. Manager Go. Consulté le 19 avril 2025 à l'adresse <https://www.manager-go.com/gestion-de-projet/cartographie-des-risques.htm>

2.2. Stratégies de gestion des risques

Afin de faire face aux risques, une entreprise peut mettre en place quatre stratégies différentes, en s’assurant que la mise en place de l’une de ces stratégies n’excède pas l’impact de la perte potentielle que la stratégie choisie est sensée couvrir. La figure suivante reprend les quatre stratégies possibles en fonction de la sévérité des risques et leurs fréquences d’occurrence (Pierandrei, 2019).

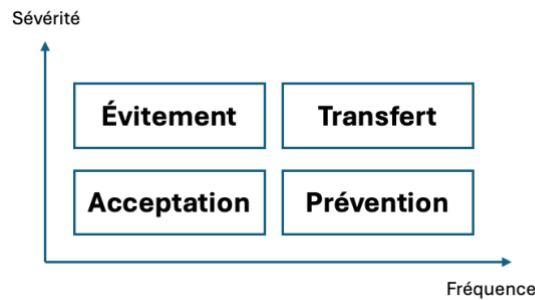


Figure 5 : L'échelle sévérité/fréquence (Pierandrei, 2019)

La première stratégie, l'acceptation, peut s'appliquer à des risques avec un faible impact sur l'entreprise et des faibles chances que ce risque se produise. Dans ce cas-ci nous décidons de ne rien faire face à ce risque et de « subir » les conséquences bien que celles-ci ne soient que modérées. Cette acceptation peut se faire notamment via des techniques d'auto-assurance, c'est-à-dire des provisions, des réserves, etc. Il est également possible de se séparer de cette partie de l'activité en la sous-traitant par exemple (Pierandrei, 2019).

L'évitement est une stratégie qui peut être utilisée lorsque les chances pour que le risque se réalise sont assez faibles, mais que la réalisation de celui-ci pourrait avoir des conséquences graves sur l'entreprise. Cette stratégie consiste tout simplement à s'éloigner du risque étant donné que si nous ne nous exposons pas au risque, il ne surviendra pas. Ceci peut se faire en éliminant les sources de facteurs à risques, en cessant des activités, des transactions ou des expositions à des opérations risquées ou encore en vendant des actifs comportant des risques (Pierandrei, 2019).

Une autre stratégie, la prévention, consiste à combattre le risque lorsque celui-ci a de plus grandes chances de se produire mais que la sévérité de la réalisation de ce risque est limitée. Ceci peut notamment se faire en mettant en place un contrôle interne rigoureux, en mettant en place des indicateurs qui sont suivis de manière régulière et en modifiant immédiatement les défaillances. Il est également important de former les équipes à la gestion de ces risques et d'avoir une communication claire sur ceux-ci (Pierandrei, 2019).

La dernière stratégie consiste tout simplement à transférer le risque à un tiers lorsque les chances de réalisations de ces risques sont grandes et que la sévérité de ceux-ci est élevée. Nous nous exposons alors totalement au risque et la perte pourrait être importante voire totale. Ces risques peuvent être couverts avec des polices d'assurance ou de réassurance etc. (Pierandrei, 2019).

2.3. Référentiels

Il existe divers cadres de référence permettant d'évaluer et de règlementer la gestion des risques d'une entreprise. Dans la suite de ce travail, nous développerons les deux référentiels les plus répandus.

2.3.1. *COSO ERM (Enterprise Risk Management)*

L'Enterprise Risk Management (ERM) est un cadre de gestion des risques ayant pour objectif d'identifier les causes et conséquences d'évènements porteurs de risques, d'en étudier l'impact sur les objectifs, le patrimoine et la performance de l'entreprise, mais également de suggérer des mesures adaptées dans le but de gérer ces risques de la meilleure manière possible (Pierandrei, 2019).

Le cadre COSO ERM, également connu comme étant le COSO II est né au début des années 2000. Il est l'évolution du cadre COSO I (cf. Chapitre 3), un référentiel dédié au contrôle interne. Cette évolution est due à l'éclatement de la bulle internet et à la croissance du nombre de faillites frauduleuses. Le COSO ERM, dédié à la gestion des risques, est donc un prolongement du COSO I, et positionne le contrôle interne comme une composante de la gestion des risques. Au contraire, le COSO I considère la gestion des risques comme étant une composante du contrôle interne (Cordel, 2019).



Figure 6 : Les huit composantes de la gestion des risques

Source : Riskforum.nl. (s.d.). COSO II. Consulté le 19 avril 2025 à l'adresse <https://riskforum.nl/encyclopedia/coso-ii/>

Comme nous pouvons le constater sur la figure ci-dessus, le COSO ERM est divisé en 8 composantes. Ces composantes reprennent les cinq composantes du cadre COSO I, mais également la « définition des objectifs », « l'identification des évènements » et la « réponse au risque ». Dans ce chapitre, nous ne développerons que les trois dernières composantes, étant donné que les cinq autres seront développées dans le chapitre dédié au contrôle interne.

Définition des objectifs

Il existe quatre grandes catégories d'objectifs retenues par le COSO, théoriquement déclinées dans l'ensemble de l'organisation, et sont généralement traduites dans les objectifs assignés aux individus, dépendant de leur niveau de responsabilité (Cordel, 2019).

Les **objectifs stratégiques** sont basés sur la vision et les missions définies par l'entreprise. Ils sont l'image des choix de la direction concernant la manière dont l'entreprise crée de la valeur. Ce sont en d'autres termes les objectifs long terme de l'entreprise (Cordel, 2019).

Les **objectifs opérationnels** permettent en quelque sorte d'atteindre les objectifs stratégiques. Ils concernent l'efficacité et l'efficience de l'organisation et sont par exemple des objectifs de rentabilité ou encore des objectifs de performance (Cordel, 2019).

Les **objectifs de reporting** ont pour but de s'assurer de la fiabilité des états financiers de l'organisation afin que la direction et les employés, mais également les autres parties prenantes, soient capables de prendre des décisions sur la base d'informations correctes (Cordel, 2019).

Finalement, les **objectifs de conformité** sont là pour faire en sorte que l'entreprise respecte les réglementations et les lois en vigueur (Cordel, 2019).

Identification des événements

L'identification des événements consiste tout simplement à identifier les événements qui pourraient avoir un impact négatif sur la création de valeur au sein de l'entreprise, en d'autres termes, qui empêcheraient l'entreprise d'atteindre ses objectifs. Il existe de nombreuses manières d'identifier ces risques telles que l'approche « bottom up » (collecter la vision des opérationnels et faire remonter à la direction) et « top down » (collecter la vision des dirigeants et partager cela à tous les niveaux), ou encore l'approche inductive (partir des causes pour identifier les effets) ou déductive (partir des conséquences pour en déduire les causes) (Cordel, 2019).

Réponses au risque

Les réponses aux différents risques identifiés ont déjà été développées dans le point précédent (cf. Chapitre 2.2.). Cette composante du COSO ERM a pour objectif d'intégrer les décisions de gestion de risques dans les processus stratégiques et opérationnels afin de les aligner avec la tolérance (l'appétence) au risque de l'entreprise, ses ressources disponibles ainsi que ses objectifs (Cordel, 2019).

2.3.2. ISO 31000

L'ISO 31000 a été émise par l'ISO (International Organization for Standardization) en 2009. C'est un référentiel conçu pour la gestion des risques et qui se rapproche fortement du COSO ERM, bien que l'ISO 31000 apporte tout de même quelques nuances (Cordel, 2019). Premièrement, la norme ISO 31000 établit un lien plus clair entre la gestion du risque et la prise de décision. De plus, la norme ISO 31000 met en avant l'importance des facteurs humains et culturels dans la gestion des risques. Finalement, la norme ISO 31010 vient compléter la norme ISO 31000 en dressant une vue d'ensemble des méthodes de quantification des risques (Cordel, 2019).

2.4. Limites de la gestion de risques

La gestion des risques est un pilier incontournable de la gestion des organisations bien que ce processus présente certaines limites. Celles-ci proviennent tant du processus de définition des objectifs, des influences sociales, de la cartographie des risques, que des heuristiques et biais cognitifs (Cordel, 2019).

2.4.1. *Limites du processus de définition des risques*

L'efficacité de la définition des risques peut être limitée par le fait qu'il est parfois difficile de réconcilier les objectifs de l'entreprise et les objectifs personnels. Les objectifs d'une entreprise sont en général transmis aux personnes chargées de les mettre en œuvre. Cette méthode se base sur plusieurs présupposés tels que le fait que la stratégie de l'organisation soit clairement définie, expliquée, acceptée et respectée de tous. La structure de l'organisation doit également être dénuée d'ambiguïté mais il faut également que les membres de l'organisation adhèrent à ses objectifs et appliquent ceux qui leur sont attribués (Cordel, 2019).

L'organisation peut également devoir faire face à des objectifs contradictoires, qui peuvent parfois se refléter dans les objectifs transmis aux individus. Certains objectifs sont également contradictoires par nature. Il faut dans ce cas ne pas aggraver la contradiction et être transparent quant à la manière dont l'organisation réalise ses choix (Cordel, 2019).

Une autre limite pouvant être rencontrée lors de la définition des risques est la définition d'objectifs irréalistes. Ce sont des objectifs inatteignables, compte tenu des moyens donnés aux personnes censées les atteindre. Des études menées par le COSO (Committee of Sponsoring Organizations of the Treadway Commission) et l'ACFE (Association of Certified Fraud Examiners) démontrent que des objectifs irréalistes constituent la principale cause du « white collar crime¹ » (Cordel, 2019).

Une mauvaise communication des objectifs peut également être une limite à la bonne gestion des risques. Bien que les objectifs de l'organisation puissent être très clairs pour les personnes les ayant définis, il faut tout de même assurer une bonne communication de ceux-ci au reste des

¹ Criminalité en col blanc. Crimes non violents commis dans un cadre professionnel par des personnes occupant des postes à responsabilité. Ex. : corruption, fraude, ... (Sengün & Partners, 2025).

employés afin qu'ils entendent les objectifs de la même manière que ceux qui les ont définis (Cordel, 2019).

Les objectifs définis peuvent également être autosuffisants, résultant dans des actions exécutées, non pas pour accomplir une tâche, mais tout simplement parce qu'il est bien vu de faire quelque chose. Ce type de situation peut arriver lorsqu'il y a des moyens sous-utilisés, entraînant certains acteurs à faire des actions déconnectées de tout objectif. Ceci peut également arriver lorsqu'une entreprise subit une forte phase de restructuration, etc. (Cordel, 2019).

Finalement, un objectif non quantifiable peut également faire émerger des limites dans la gestion des risques. En effet, dans le cas où un degré d'atteinte des objectifs ne peut pas clairement se mesurer, l'objectif ne sera pas ou peu quantifiable (Cordel, 2019).

2.4.2. Les influences sociales

Les influences sociales peuvent avoir un impact sur la gestion des risques au sein d'une organisation. En effet, bien que dans la majorité des cas, des décisions de groupes produisent un meilleur résultat qu'une décision prise isolément par un individu, l'inverse est également possible et c'est ce que nous pouvons appeler des « décisions absurdes ». Des psychologues sociaux ont identifié divers mécanismes d'influence au sein de groupes tels que la paresse sociale, le conformisme et la polarisation de groupe. La paresse sociale désigne le fait qu'un individu fournira moins d'efforts lorsqu'il est en groupe que s'il est seul. Le conformisme désigne le fait qu'un individu modifie son comportement pour se conformer au reste du groupe dans le but d'être accepté. La polarisation est une autre forme de conformisme et désigne la tendance de l'extrémisation des réponses initialement présentes chez un individu au sein d'un groupe (Cordel, 2019).

2.4.3. La cartographie des risques

La cartographie des risques comprend également des limites telles que la problématique de la compression des intervalles ou encore la problématique de la corrélation entre les risques (Cordel, 2019).

La compression d'intervalles correspond au fait que dans la cartographie des risques, des échelles sont utilisées pour classifier les risques en fonction de leur probabilité et de leur impact. Le problème est qu'il y a en moyenne 5 graduations, ce qui signifie que des risques dont la probabilité et l'impact varient fortement entre eux, se retrouvent parfois classés au même niveau. Cet effet est encore davantage amplifié par la multiplication des deux facteurs (impact, probabilité). La représentation cartographique n'est donc parfois pas la plus adaptée (Cordel, 2019).

La plupart des cartographies ne prennent, en général, pas en compte la corrélation qu'il peut y avoir entre plusieurs risques. En d'autres termes, nous faisons l'hypothèse que les risques sont indépendants les uns des autres ce qui peut être une vision erronée de la réalité (Cordel, 2019).

2.4.4. Les heuristiques et biais cognitifs

L'heuristique désigne l'utilisation de règles empiriques, pratiques, rapides et simples, permettant de faciliter l'analyse de situations dans le but de résoudre rapidement des problèmes ou de prendre des décisions. Ce sont en quelques sortes des raccourcis intellectuels développés sur base de l'expérience ou d'analogies. Il existe de nombreuses heuristiques telles que l'heuristique de représentativité, de disponibilité ou encore de l'ancrage et d'ajustement (Cordel, 2019).

Un biais cognitif est une « erreur affectant le processus de prise de décision et/ou l'attitude mise en œuvre face à une situation particulière, cette dernière étant liée à un mauvais traitement des informations disponibles » (Cordel, 2019).

3. Contrôle interne

De la même manière que pour la gestion des risques, le passé nous a déjà démontré qu'un mauvais contrôle interne pouvait avoir des conséquences désastreuses comme cela a été le cas pour la Société Générale et l'affaire Jérôme Kerviel en 2008. Nous verrons dans cette partie ce que nous entendons par contrôle interne, comment il est mis en place, mais également ses limites.

3.1. Définition

Le contrôle interne est un processus mis en place dans les entreprises par le conseil d'administration, les dirigeants ainsi que le personnel et dont l'objectif est de fournir une assurance raisonnable quant à la réalisation et l'optimisation des opérations, la fiabilité des informations financières, mais également la conformité aux lois et aux règlements en vigueur (Cordel, 2019).

En plus de ces objectifs de gestion des risques, d'exactitude des informations, de conformité et de l'optimisation des opérations, il est important que le contrôle intègre une certaine séparation des tâches. L'objectif de la séparation des tâches est d'attribuer à des personnes différentes des activités de contrôle spécifiques dans le but d'empêcher qu'une personne ait un contrôle exclusif et excessif et qu'elle utilise ce pouvoir à des fins préjudiciables ou illégales. Il faut articuler à cela le principe de « besoin de savoir », autrement dit, donner accès à certaines informations uniquement si cela est nécessaire à la réalisation de leur mission respective (Edlinger, I, 2025).

Le contrôle interne contribue à la prévention et la gestion des risques de ne pas atteindre les objectifs que l'organisation s'est fixée. Il joue également un rôle important dans le pilotage et la conduite des différentes activités d'une organisation (AMF, 2010).

Comme mentionné ci-dessus, l'implémentation d'un contrôle interne est fortement recommandée pour toute entreprise, peu importe sa taille et son secteur d'activité, compte tenu des bénéfices que cela apporte à l'entreprise. Toutefois, l'implémentation d'un contrôle interne est obligatoire pour certaines entreprises telles que les institutions financières, les entreprises d'assurances et de réassurances, mais également les entreprises cotées ainsi que les entités d'intérêt public et les pouvoirs fédéraux en Belgique (cf. infra p.20).

Le renforcement des réglementations concernant le contrôle interne en Belgique vient de l'adoption de la Loi Sabarnes-Oxley (SOX) aux États-Unis en 2002. Bien que cette loi soit américaine, elle a fortement influencé la gestion de risques et le contrôle interne à l'échelle mondiale. Cette loi a été votée à la suite de scandales financiers tels que Enron ou Worldcom. Elle a pour objectif de « protéger les investisseurs en améliorant l'exactitude et la fiabilité des informations publiées par les entreprises » (Cordel, 2019).

Cette loi est novatrice aux États-Unis car elle oblige les sociétés cotées à publier un rapport signé par le directeur général ainsi que le directeur financier, concernant l'évaluation du contrôle interne (section 404a de la loi) et à la certification de ce rapport par des auditeurs externes (section 404b de la loi). Cette loi a également un effet extraterritorial car elle s'applique aux sociétés cotées, américaines, mais également aux filiales de sociétés, américaines ou non, cotées aux États-Unis. Les articles 302 et 404 (a et b) traitent directement du contrôle interne (Cordel, 2019).

D'un point de vue européen, la loi SOX a également influencé son cadre réglementaire. Deux directives européennes traitent directement du contrôle interne : la directive européenne 2006/46/CE et la directive européenne 2006/43/CE (Cordel, 2019).

Directive européenne 2006/46/CE

Cette directive stipule que « toute société dont les titres sont admis à la négociation sur un marché réglementé doit inclure une déclaration sur le gouvernement d'entreprise dans son rapport de gestion. Cette déclaration forme une section spécifique du rapport de gestion et contient une information des principales caractéristiques des systèmes de contrôle interne et de gestion des risques de la société dans le cadre du processus d'établissement de l'information financière » (Cordel, 2019).

Directive européenne 2006/43/CE

Cette directive stipule qu'un comité d'audit doit obligatoirement être mis en place car celui-ci permet de réduire les risques financiers, opérationnels et de non-conformité. Cet article définit également les missions du comité d'audit (Cordel, 2019) :

- Suivi du processus d'élaboration de l'information financière
- Suivi de l'efficacité des systèmes de contrôle interne, d'audit interne et de gestion des risques
- Suivi du contrôle légal des comptes annuels et des comptes consolidés.
- Examen et suivi de l'indépendance du contrôleur légal des comptes ou du cabinet d'audit

(Cordel, 2019).

En Belgique, diverses lois et arrêtés régissent la réglementation du contrôle interne. La directive européenne est transposée dans la loi belge par la loi du 7 décembre 2016 portant sur l'organisation de la profession et de la supervision publique des réviseurs d'entreprise. Cette loi stipule que les entreprises d'intérêt public doivent mettre en place des mécanismes de contrôle interne afin de garantir la fiabilité des informations financières (Loi du 7 décembre 2016, Moniteur belge)

Par entité d'intérêt public, il faut entendre :

- Les sociétés cotées
- Les établissements de crédit
- Les entreprises d'assurance ou de réassurance
- Les organismes de liquidation et organismes assimilés à des organismes de liquidation

(Loi du 7 décembre 2016, Moniteur belge)

Les pouvoirs locaux belges sont également soumis à l'obligation de la mise en place d'un contrôle interne. L'arrêté royal du 17 août 2007 relatif au contrôle interne et la gestion des risques au sein des services publics fédéraux impose des normes minimales auxquelles les structures de contrôle interne, d'audit interne et d'évaluation, doivent répondre. Cet arrêté impose entre autres la mise en place d'un système de contrôle interne fondé sur le COSO, une séparation claire des pouvoirs, la traçabilité des opérations, la mise en place de mécanismes d'évaluation et de correction mais également l'obligation pour les dirigeants d'en rendre compte (Arrêté royal du 17 août 2007, Moniteur belge).

3.2. Lignes de défense

Il existe 3 lignes de défense, permettant d'organiser la gestion des risques, du contrôle interne et de la gouvernance dans une entreprise. Elles définissent la répartition claire des rôles et responsabilités sur trois niveaux complémentaires.

La première ligne de défense, correspondant à la gestion opérationnelle, a des rôles directement liés à la livraison de produits et/ou services aux clients d'une organisation mais est également en première ligne pour la gestion des risques liés aux activités. Sa proximité avec le terrain lui permet d'identifier rapidement des problèmes ou des anomalies. C'est la première ligne de défense qui est responsable d'appliquer de manière active un contrôle interne (IIA, 2020).

La deuxième ligne de défense, correspondant aux fonctions de contrôle, comprend les rôles de support à la gestion des risques et est là pour encadrer la première ligne de défense. Certaines activités de la deuxième ligne de défense peuvent être confiées à des spécialistes. La deuxième ligne de défense joue donc un rôle de supervision et de coordination et assure que les risques identifiés par la première ligne de défense soient suivis de manière rigoureuse (IIA, 2020).

La troisième ligne de défense concerne l'audit interne. Les personnes chargées de l'audit interne doivent être indépendantes de la direction afin de garantir son objectivité. L'objectif d'un audit interne est de mettre en place des contrôles afin de s'assurer de l'adéquation et de l'efficacité de la gestion des risques et du contrôle interne mis en place au sein de l'organisation. Ils donnent l'assurance indépendante et raisonnable que les objectifs définis par l'organisation soient atteints (IIA, 2020).

En résumé, la première ligne de défense est responsable d'appliquer un contrôle interne afin de s'assurer que les objectifs définis peuvent être atteints, tandis que la deuxième ligne de défense est là en tant que support à la première ligne de défense. La troisième ligne de défense évalue et audite de manière indépendante les contrôles mis en place afin de voir s'ils sont efficaces.

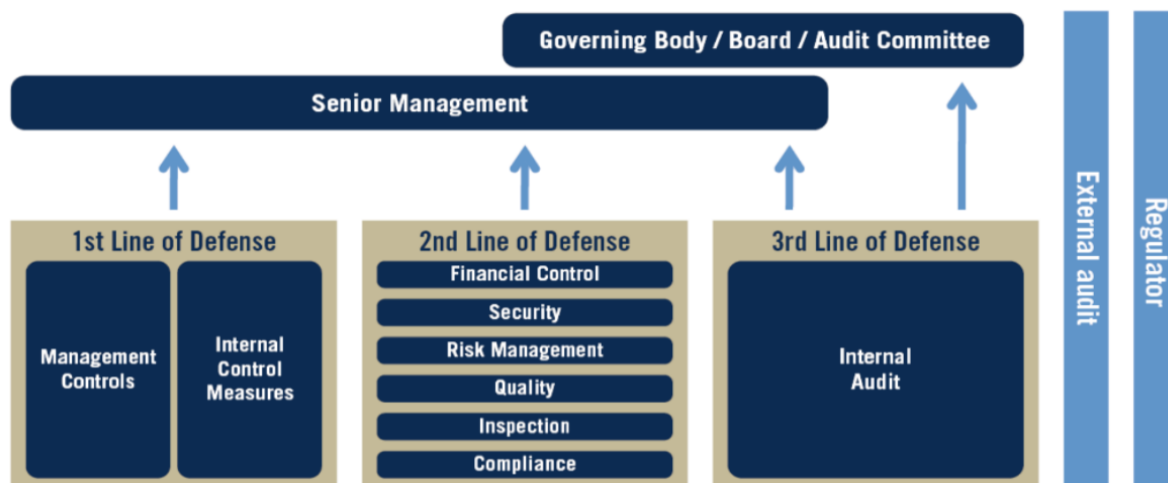


Figure 7 : Modèles des trois lignes de défense

Source : Steinmetz, T. (2020). *Gestion des risques en entreprise : Le système des trois lignes de défense et ses détracteurs*. [Travail de fin d'études]. Louvain School of Management.

3.3. Référentiel – COSO

Le COSO I (COSO Internal Control Integrated Framework), élaboré par le COSO (Committee of Sponsoring Organizations of the Treadway Commission) en 1992 et revu en 2013, est un référentiel de contrôle interne, servant de base pour documenter et évaluer le contrôle interne. Le contrôle interne est un processus itératif, dynamique et intégré où chaque élément s'applique aux trois objectifs et ce processus est propre à chaque entreprise (Cordel, 2019).

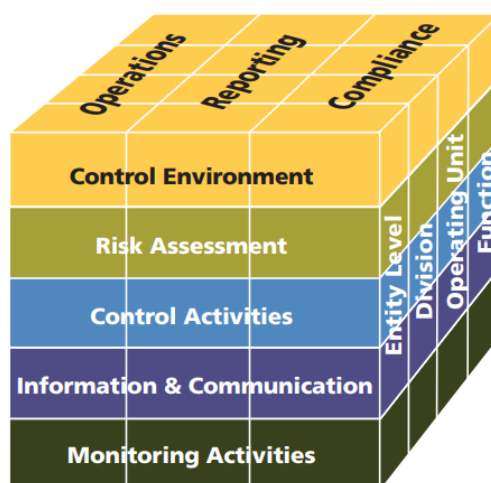


Figure 8 : COSO I

Source : KnowledgeLeader. (2020). Five Components of the COSO Framework You Need to Know. Consulté le 21 avril 2025 à l'adresse <https://info.knowledgeleader.com/bid/161685/what-are-the-five-components-of-the-coso-framework>

3.3.1. Objectifs de contrôle

Le COSO I est articulé autour des trois objectifs de contrôle interne que doit atteindre une organisation : la réalisation et l'optimisation des opérations, la fiabilité des informations financières et de gestion ainsi que la conformité aux lois et aux réglementations en vigueur (Cordel, 2019).

3.3.2. Niveaux de responsabilités

Le contrôle interne est conçu et appliqué à différents niveaux de responsabilité organisationnels, permettant d'ancrer les mécanismes de contrôle interne à l'ensemble de l'organisation. (Cordel, 2019).

3.3.3. Éléments de contrôle

Finalement, le COSO I est composé de 5 éléments de contrôle articulés autour de 17 principes de base, permettant un contrôle interne efficace ainsi qu'un soutien à l'organisation dans la réalisation de ses objectifs (Cordel, 2019).

Pour garantir une efficacité du contrôle interne, le cadre COSO de 2013 exige que les cinq éléments soient présents (qu'ils existent) et fonctionnels, mais également que ces éléments fonctionnent de manière intégrée (Dugal et al., 2013).

Environnement de contrôle (Control Environment)

« L'environnement de contrôle désigne l'ensemble des normes, processus et des structures essentielles pour l'exécution des contrôles internes à l'échelle de l'entité. Le conseil d'administration et la haute direction donnent l'exemple venant de l'échelon supérieur quant à l'importance du contrôle interne et aux normes de conduite attendues. » Cette composante regroupe cinq principes (Dugal et al., 2013) :

1. L'entité s'engage en faveur des valeurs éthiques et de l'intégrité.
2. Le conseil d'administration prouve qu'il est indépendant de la direction et surveille l'élaboration et l'exécution des contrôles internes.
3. La direction établit les structures, la hiérarchie et la délégation des pouvoirs et responsabilités dans le but d'atteindre les objectifs, et ce, sous la supervision du conseil.
4. L'organisation montre sa volonté d'attirer, de former et de fidéliser les ressources requises pour atteindre les objectifs fixés.
5. L'organisation tient les personnes responsables des contrôles internes dans le but d'atteindre les objectifs.

(Dugal et al., 2013).

Évaluation des risques (Risk Assessment)

L'évaluation des risques est un processus itératif de détection et d'analyse des risques qui sont susceptibles d'avoir un impact négatif sur l'atteinte des objectifs fixés par l'organisation. La direction doit tenir compte des évolutions contextuelles externes ainsi que des évolutions internes à l'organisation pouvant exercer une influence sur l'atteinte des objectifs. Cette composante regroupe quatre grands principes (Dugal et al., 2013) :

6. L'entité définit de manière suffisamment claire ses objectifs, permettant la détection et l'évaluation des risques.
 7. L'entité identifie, évalue et analyse les risques pouvant compromettre l'atteinte des objectifs fixés, dans le but de définir une stratégie appropriée pour gérer ces risques.
 8. L'entité prend en considération la possibilité de fraudes lors de l'évaluation des risques.
 9. L'entité identifie et évalue les changements significatifs pouvant avoir un impact sur le système de contrôle interne.
- (Dugal et al., 2013).

Activités de contrôle (Control Activities)

Les activités de contrôle sont des actions établies à travers des politiques et procédures visant à s'assurer que les directives, émises par la direction en vue d'atténuer les risques pouvant compromettre l'atteinte des objectifs, soient mises en œuvre. Ces activités de contrôle doivent être exécutées à tous les niveaux de l'entité, et ce, lors des différentes étapes du processus opérationnel. Ces actions peuvent tant être préventives que détectives, mais peuvent également être manuelles ou automatisées, dépendant de l'action mise en place. La séparation des pouvoirs est l'une des activités de contrôle essentielles. Cette composante comprend les trois grands principes suivants. (Dugal et al., 2013) :

10. L'entité sélectionne et développe des activités de contrôle contribuant à la réduction du niveau des risques pouvant compromettre l'atteinte des objectifs à un niveau considéré comme étant acceptable par l'entité.
 11. L'entité sélectionne et développe des activités de contrôle général sur la technologie afin de favoriser l'atteinte des objectifs.
 12. L'entité développe des activités de contrôle à travers des politiques qui établissent ce qui est attendu mais également à travers des procédures mettant ces politiques en œuvre.
- (Dugal et al., 2013).

Information et communication (Information and Communication)

Les informations sont cruciales pour que l'entité puisse exercer ses responsabilités en matière de contrôle interne afin de réaliser ses objectifs. La communication est un processus continu et itératif consistant à fournir à l'entité les informations nécessaires afin d'exécuter ses activités de contrôle interne au quotidien. Cette communication permet une compréhension des responsabilités de chacun, mais également de mesurer leur importance dans le but d'atteindre des objectifs. L'information et la communication reposent sur trois principes (Dugal et al., 2013) :

13. L'entité obtient ou génère des informations pertinentes et qualitatives qu'elle utilise pour soutenir le fonctionnement du contrôle interne.
 14. L'entité communique en interne les informations nécessaires, y compris les objectifs et responsabilités concernant le contrôle interne, afin de soutenir le fonctionnement du contrôle interne.
 15. L'entité communique avec les parties externes concernant les questions pouvant affecter le fonctionnement du contrôle interne.
- (Dugal et al., 2013).

Activités de suivi (Monitoring Activities)

Des évaluations continues (intégrées dans les activités habituelles), distinctes (évaluation menée périodiquement par des gestionnaires d'objectifs, membres de l'audit interne ou partenaires externes), ou une combinaison des deux sont utilisées afin de vérifier si chacune des cinq composantes du contrôle interne, en ce compris les contrôles visant à appliquer les principes de chacune des composantes, est présente et fonctionnelle. Il est important de faire remonter les constatations et déficiences rapidement à la direction et au conseil d'administration. Les activités de suivi reposent sur deux principes (Dugal et al., 2013) :

16. L'entité sélectionne, développe et effectue des évaluations continues et/ou distinctes afin de s'assurer que toutes les composantes du contrôle interne soient présentes et fonctionnelles.
17. L'entité évalue et communique les déficiences du contrôle interne aux parties chargées de prendre des mesures correctives, y compris la haute direction et le conseil d'administration, le cas échéant.

(Dugal et al., 2013).

3.4. Limites et déficiences du contrôle interne

Le contrôle interne est essentiel afin d'améliorer la gouvernance, la gestion des risques et la fiabilité des informations financières mais il ne fournit qu'une assurance raisonnable quant à la réalisation des objectifs. Il présente également certaines limites inhérentes qu'il est important de souligner telles que la part de jugement présente dans le contrôle interne, le fait que des défaillances peuvent survenir ou encore que des erreurs peuvent être faites. Il existe également la possibilité de collusion entre des employés ou la possibilité que le management déroge au système de contrôle interne. L'aspect coûts/bénéfices doit également être pris en compte (Committee of Sponsoring Organizations of the Treadway Commission (COSO), 1994).

3.4.1. Limites liées au coût

Les entreprises mettant en place un contrôle interne prendront incontestablement en considération les coûts et les bénéfices liés à sa mise en place. Elle peut être coûteuse car les entreprises doivent investir dans des ressources humaines et technologiques et mettre en place des processus. Dans certains cas, cela pourrait coûter plus cher à l'entreprise de mettre en place des procédures que de subir les conséquences d'un risque se réalisant. (COSO, 1994).

3.4.2. Limites liées au jugement

L'efficacité des contrôles internes dépend également de la capacité de l'être humain à prendre des décisions commerciales, nécessitant un jugement humain dans un temps restreint et sur base des informations disponibles. Certaines décisions humaines étant perçues comme étant les plus judicieuses peuvent, avec du recul, s'avérer être moins positives qu'espéré, nécessitant des changements par la suite (COSO, 1994).

3.4.3. Limites liées aux défaillances

Le contrôle interne peut également comporter des défaillances et des erreurs commises par les personnes responsables du contrôle. Le personnel peut commettre des erreurs de jugement ou encore commettre des erreurs d'inattention liées à la distraction ou la fatigue. Des changements dans le système pourraient également être mis en place avant même que le personnel ait été formé pour réagir de manière appropriée aux signes d'un fonctionnement incorrect (COSO, 1994).

3.4.4. Limites liées à la dérogation de gestion (Management Override)

L'efficacité d'un contrôle interne dépend entièrement des personnes responsables de son bon fonctionnement. Même dans une organisation où le contrôle interne est implémenté de manière efficace, un responsable pourrait être en mesure de passer outre le contrôle interne à des fins illégitimes afin d'en bénéficier personnellement ou dans le but d'améliorer l'image de la situation financière de l'entité. Les raisons pouvant pousser un manager à outrepasser le contrôle interne peuvent être multiples : augmenter les recettes déclarées, masquer la diminution d'une part de marché, modifier les résultats pour atteindre des budgets irréalistes, etc. (COSO, 1994).

Il ne faut tout de même pas confondre dérogation et intervention de la direction visant à écarter des procédures ou des politiques à des fins légitimes. L'intervention de la direction est nécessaire pour traiter des cas non-conventionnels qui seraient « mal » traités par les procédures mises en place initialement. L'intervention de la direction est nécessaire car aucune procédure ne peut être conçue pour anticiper tous les cas de figure auxquels elle devra faire face. Contrairement aux dérogations, les interventions de la direction sont en général documentées ou communiquées au personnel concerné (COSO, 1994).

3.4.5. Collusion

Les activités collusoires entre deux ou plusieurs individus peuvent avoir un impact sur le contrôle interne. Ces personnes peuvent modifier des données financières ou d'autres informations de gestion sans que cette modification ne soit perceptible par le contrôle interne, dans le but de d'accomplir une action et de la dissimuler. Cette collusion peut survenir entre une personne exerçant un rôle de contrôle important et un client, un fournisseur ou encore un autre employé. De la même manière, plusieurs personnes peuvent se mettre d'accord afin de contourner les contrôles internes mis en place (COSO, 1994).

4. Intelligence Artificielle

4.1. Définition

L'intelligence artificielle (IA) est un concept vaste à définir car il comprend à la fois la notion d'intelligence mais également sa nature multidisciplinaire. L'intelligence fait allusion à la capacité d'apprentissage, de mémorisation, de communication, d'adaptation, de décision, de représentation des connaissances mais englobe également la perception et la réflexion. L'intelligence artificielle en tant que telle regroupe de nombreuses disciplines telles que l'informatique, les mathématiques, les sciences cognitives et est soutenue par la psychologie, la philosophie, les neurosciences, etc. C'est donc la raison pour laquelle seul un modèle complexe est capable de représenter la qualification artificielle de cette intelligence (Fuhrer, 2023).

Afin d'apporter des nuances à cette définition, il est intéressant de se pencher sur des approches plus générales du concept, vulgarisant certains aspects et facilitant ainsi la compréhension.

L'OCDE (Organisation de Coopération et de Développement Économiques) définit l'intelligence artificielle (IA) comme étant « un système basé sur une machine qui peut, pour un ensemble donné d'objectifs définis par l'homme, faire des prédictions, des recommandations ou des décisions influençant des environnements réels ou virtuels » (The Organisation for Economic Co-operation and Development (OECD), 2019).

Le dictionnaire Le Robert définit l'intelligence artificielle comme suit : « Ensemble des théories et des techniques développant des programmes informatiques complexes capables de simuler certains traits de l'intelligence humaine (raisonnement, apprentissage...) » (Le Robert, s.d.).

Le Parlement Européen a défini l'intelligence artificielle (IA) comme étant la capacité d'une machine à reproduire des comportements semblables à ceux des humains tant dans son raisonnement, que sa créativité ou encore la planification (Parlement européen, 2023).

Les définitions pour l'IA sont nombreuses mais toutes convergent vers une même idée : c'est la capacité d'un système d'apprendre de manière autonome et de restituer des informations sur base de son environnement et de requêtes, d'une manière semblable à celle d'un humain. Nous nous baserons sur cette dernière définition lorsqu'il sera question d'IA dans la suite de ce travail.

4.2. Histoire

Bien que le terme « Intelligence Artificielle (IA) » pourrait paraître assez récent, ses prémices sont en réalité bien plus anciennes. C'est à la fin de la Seconde Guerre mondiale, dans les années 1950, que des chercheurs avant-gardistes ont la volonté de créer une technologie capable d'imiter l'intelligence humaine. Nous sommes à ce moment là encore loin des technologies que nous connaissons aujourd'hui bien que l'objectif soit déjà clairement défini : créer un système capable d'apprendre de manière autonome et résoudre des problèmes complexes (Brenet, 2024).

C'est donc en 1950 qu'Alan Turing posera les bases de ce qui deviendra dans le futur l'intelligence artificielle telle que nous la connaissons aujourd'hui. Il publiera son essai « Computing Machinery and Intelligence », traitant de la capacité des machines à penser, illustré par le Test de Turing (Brenet, 2024).

L'idée du Test de Turing est de mettre en opposition un être humain (B) et un ordinateur (A). Un autre être humain (C) interagit avec eux à l'aide de texte, sans savoir qui est à l'origine de quelle réponse renvoyée. L'objectif est de voir si l'humain est capable d'identifier qui est l'humain et qui est l'ordinateur. En d'autres termes, est-ce qu'un être humain est capable d'identifier s'il discute avec un autre être humain ou avec un ordinateur. S'il n'en est pas capable, cela voudrait dire que l'ordinateur est capable de penser tel un être humain et donc en quelque sorte, qu'il s'agisse d'une certaine forme d'intelligence artificielle (University of Oxford, 2023). L'image ci-après illustre ce test.

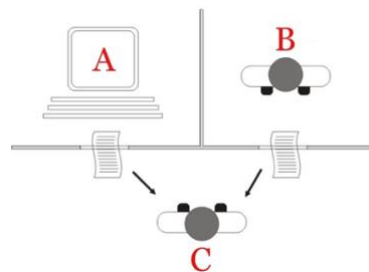


Figure 9: Test de Turing

Source : Wikipédia. (2025). Test de Turing. Consulté le 30 mars 2025 à l'adresse https://fr.wikipedia.org/wiki/Test_de_Turing

En 2011, Watson, un ordinateur développé par IBM, remporte « Jeopardy », un jeu télévisé américain portant sur la culture générale. Dans ce jeu, trois candidats doivent trouver la question correcte à une réponse donnée. C'est un jeu de rapidité, mais également de gestion de risques. En effet, une bonne réponse fait gagner de l'argent, mais une mauvaise réponse fait perdre de l'argent (Niederborn, 2019).

Pour développer Watson, IBM a procédé à l'analyse des stratégies des meilleurs joueurs de Jeopardy. Watson est en réalité un assemblage de 90 serveurs, regroupant l'équivalent de 1 million de livres d'informations concernant la culture générale (encyclopédies, romans, dictionnaires, ...). Il a été entraîné sur 55 sessions de tests face à d'anciens joueurs, lui permettant d'apprendre de ses erreurs et d'identifier les subtilités et les pièges des questions. Il n'était pas parfait, mais l'objectif était de battre les deux meilleurs joueurs du jeu et non pas d'être infaillible (Niederborn, 2019).

Depuis lors, Watson a été assigné à de nombreuses autres tâches telles que de la médecine. Il a été entraîné à identifier des cas de cancers sur base de diagnostics et en 2016, sur base de 1000 cas soumis à Watson, 99% de ses diagnostics correspondaient à celui des médecins bien que dans 30% des cas, son diagnostic était basé sur une lecture que les médecins n'avaient pas faite. Il aide également les employés du Crédit Mutuel, une banque en France, à trier leurs courriers électroniques (Niedercorn, 2019).

En 2016, DeepMind, une filiale de Google, crée le programme AlphaGo. C'est un programme développé pour battre le champion du monde de Go, un jeu de plateau d'origine chinoise et réputé pour sa complexité. L'objectif est atteint car AlphaGo bat le meilleur joueur de Go de l'époque et réussit même à exploiter des techniques qui n'avaient quasiment jamais été utilisées, inspirant au passage les joueurs de Go. AlphaGo est la preuve qu'un ordinateur est capable de comprendre et de maîtriser les techniques d'un jeu extrêmement complexe (Google Deep Mind, s.d.).

2015 marque la fondation d'une entreprise qui révolutionnera le domaine de l'intelligence artificielle et le rendra accessible au grand public, OpenAI. C'est une entreprise américaine fondée par des leaders en technologie, notamment Elon Musk et Sam Altman. Leur objectif était de rendre accessible l'IA et que cela profite à l'humanité (Heienickle, 2024).

Trois ans après, GPT-1 (Generative Pre-Trained Transformer) sort et comporte 117 millions de paramètres. GPT-1 démontre qu'une machine est capable d'intégrer un texte et d'en prédire la suite et sert de base pour les versions ultérieures. Au mois de février 2019, GPT-2 est développé et compte pas moins de 1,5 milliard de paramètres mais il ne sera rendu public que quelques mois plus tard par crainte d'usage abusif. Il est capable de générer des réponses qui ont du sens. GPT-3, lancé en 2020, bouleverse davantage les utilisateurs car il est capable de bien plus de choses que ses prédécesseurs telles que la rédaction d'articles ou de poésie ou encore de répondre à des questions. Cette version de GPT était dotée de plus de 175 milliards de paramètres (Heienickle, 2024).

C'est finalement en 2023 que GPT-4 est lancé, une version bien plus avancée que les précédentes, capable d'analyser du texte, des images et de mieux comprendre les requêtes de ses utilisateurs. Bien qu'avec la troisième version de GPT, le monde a commencé à comprendre l'utilité que pouvait avoir ChatGPT dans la vie de tous les jours, c'est avec la quatrième version que son usage se démocratise et que l'utilisation de l'intelligence artificielle par le grand public explose. Depuis sa création, la croissance de ChatGPT-4 a été exponentielle, comptant plus de 100 millions d'utilisateurs seulement deux mois après son lancement. Ceci est la preuve qu'un besoin existait auprès du public pour ce genre de produits. Le graphique figurant dans l'annexe 1 illustre la croissance de ChatGPT-4 depuis son lancement en 2023 (Heienickle, 2024).

ChatGPT voit de nos jours de nombreux concurrents apparaître tels que Copilot (Microsoft) ou encore Gemini (Google). De nombreuses entreprises développent également leur propre IA générative afin de l'adapter à leurs besoins et d'y intégrer des restrictions comme l'a par exemple fait JPMorgan Chase & Co, une banque américaine ayant développé sa propre IA spécialisée dans le conseil financier (Son, 2023).

4.3. Types d'Intelligences Artificielles

Il existe deux principales sortes d'intelligences artificielles, les IA « faibles » et les IA « fortes ». Celles-ci sont fondamentalement différentes, tant dans leurs conceptions que de leurs applications.

Une IA faible, également appelée IA étroite, est un système conçu dans le but de réaliser une seule tâche bien précise de manière intelligente. L'IA faible est donc capable de reproduire le comportement humain mais est fortement limitée quant au nombre tâches qu'elle sera capable d'accomplir. C'est un système expert dans son domaine, incapable de généraliser son apprentissage à d'autres domaines (Brenet, 2024). Une IA faible se base sur une entrée humaine pour définir ses algorithmes d'apprentissage et ses paramètres ainsi que pour son alimentation en données pertinentes pour garantir sa précision (IBM, 2021).

Voici quelques exemples d'IA faibles :

- Les systèmes de recommandations
- Les assistants virtuels (Siri, Amazon Alexa, ...)
- Les voitures à conduite autonome
- Les systèmes de reconnaissance faciale
- ...

(Brenet, 2024)

Au contraire, une IA forte ou IA générale (AGI) est une forme théorique utilisée pour décrire un certain état d'esprit en matière de développement de l'IA (IBM, 2021). Une IA forte est capable d'imiter l'intelligence humaine dans son « ensemble ». Ce sont des systèmes capables de comprendre, de raisonner, d'apprendre et d'effectuer des tâches complexes de la même manière que le ferait un être humain (Brenet, 2024).

Contrairement à une IA faible, une IA forte est dotée d'un système complexe d'apprentissage (capacité cognitive) permettant à la machine de s'améliorer en permanence mais surtout d'apprendre de ses erreurs. Elle est censée être capable de résoudre tout type de problème (Brenet, 2024).

Malgré des investissements considérables de la part des chercheurs, tant dans le secteur privé que le milieu universitaire, l'IA forte ne reste aujourd'hui encore qu'un concept théorique et non un produit abouti et fonctionnel. Les avis concernant cette technologie divisent avec d'une part, des personnes optimistes et confiantes qu'une telle technologie sera dévoilée dans un futur plus ou moins proche, et d'autre part, des personnes plus pessimistes, convaincus que l'IA forte ne verra jamais le jour (IBM, 2021).

Il faut tout de même savoir que le domaine de l'IA évolue rapidement et d'autres technologies voient le jour telles que la « Superintelligence Artificielle (ASI) ». Cette IA devrait dépasser l'IA forte en termes d'intelligence et de capacités humaines mais celle-ci reste cependant purement spéculative étant donné que l'IA forte n'est elle-même pas encore aboutie (IBM, 2021).

4.4. Les modèles d'Intelligence Artificielle : Le Machine Learning

Il existe différents modèles d'intelligence artificielle permettant à des systèmes de simuler des formes d'intelligence humaine. Chacun de ces modèles distincts contribue à l'avancement de l'IA et ouvre des voies à des applications que l'on peut considérer aujourd'hui encore comme révolutionnaires. Le schéma ci-dessous représente de manière visuelle et synthétique comment ces modèles sont liés entre eux (Brenet, 2024).

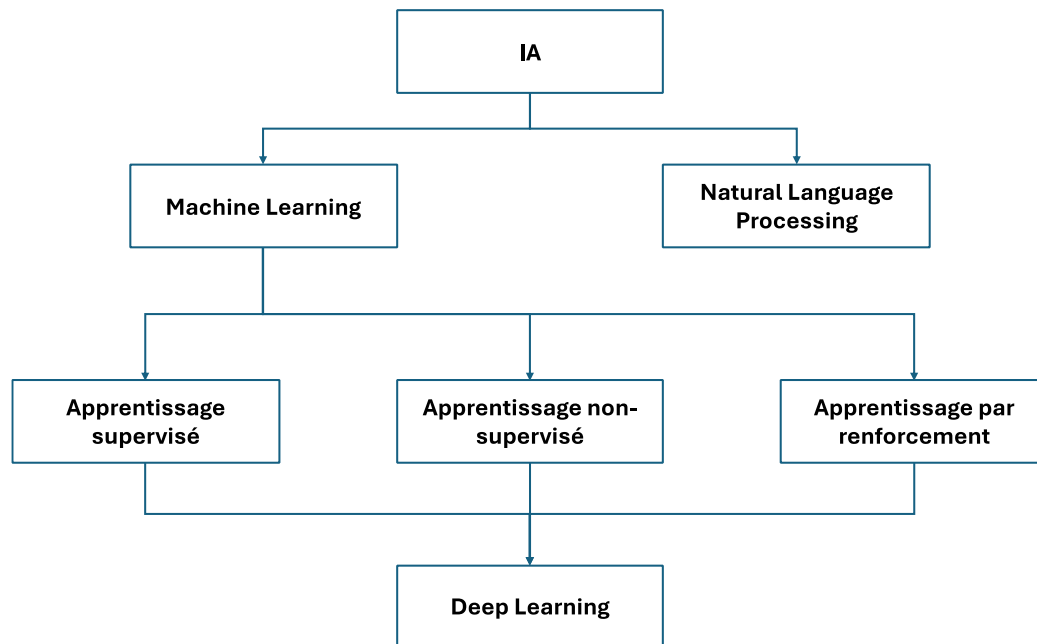


Figure 10 : Les modèles d'Intelligence Artificielle (Brenet, 2024).

4.4.1. Machine Learning (ML)

Le Machine Learning est l'une des branches principales de l'IA. C'est une approche technologique révolutionnaire qui permet à des data scientists² d'alimenter des algorithmes avec des données, permettant ainsi aux machines d'apprendre et de prendre des décisions sans pour autant que cela ait été programmé. Cela signifie que la machine ne suit plus des instructions strictes mais qu'elle est au contraire capable d'acquérir des connaissances à partir de données numériques préexistantes et de s'améliorer grâce à un apprentissage continu mais également grâce à la croissance du volume de données disponibles (Brenet, 2024).

L'utilité principale du Machine Learning est de repérer des tendances et similitudes que l'on appelle également « patterns », et ceci tant pour des images que des statistiques ou encore des mots (Brenet, 2024).

4.4.2. Les paradigmes d'apprentissage

Le premier paradigme d'apprentissage est l'**apprentissage supervisé**. C'est une approche qui a pour objectif d'élaborer des modèles de prédiction afin d'anticiper des choses telles que les besoins d'une entreprise. Dans ce cas-ci, la machine sait ce que nous attendons d'elle et notre

² Experts en données

rôle est alors de la guider dans son acquisition de connaissances en lui donnant des exemples de questions et leurs réponses. L'objectif de ce modèle est d'entraîner suffisamment le système afin qu'il soit capable de prédire les réponses correctes pour des nouvelles données non étudiées auparavant (Brenet, 2024).

Le type de données utilisées dans ce genre d'apprentissage sont dites « étiquetées », c'est-à-dire que nous donnons avec la donnée la valeur de sortie attendue. Nous lui donnons en quelque sorte la réponse à la question. Par exemple, s'il lui est demandé de trier des images, chaque image sera étiquetée avec la catégorie à laquelle elle appartient (Brenet, 2024).

L'évaluation de cette méthode d'apprentissage est assez simple car il suffit de comparer ses prédictions avec les valeurs attendues (Brenet, 2024).

Le deuxième paradigme d'apprentissage est **l'apprentissage non supervisé**. Le système est ici entraîné avec des données qui ne disposent pas d'étiquette. Le modèle va cette fois-ci se baser sur des similitudes qu'il identifiera lui-même, ce qui lui permettra ensuite de faire des regroupements appelés « clusters ». L'objectif est donc de regrouper des données similaires ou de réduire la dimensionnalité afin de faciliter l'analyse des données. Son objectif est de découvrir une structure ou des modèles dans les données que nous lui fournissons. Il est plus difficile d'évaluer un tel modèle car les réponses correctes n'ont pas été prédéfinies (Brenet, 2024).

Le dernier paradigme est **l'apprentissage par renforcement**, une méthode d'apprentissage de plus en plus répandue. Dans ce cas-ci, la machine est récompensée pour des bonnes réponses et est pénalisée dans le cas contraire. Le système doit apprendre à accomplir une tâche dans un environnement incertain et complexe. Il va essayer différentes actions et apprendre de ses erreurs. Chaque action entreprise par le système est suivie d'une récompense ou d'une pénalité et l'objectif de ce système est bien évidemment de maximiser ses récompenses. Il découvre par lui-même la stratégie la plus adéquate en fonctionnant par essai-erreur jusqu'à développer des stratégies de décision très sophistiquées. Il est important de souligner le fait que le système ne reçoit pas de consignes pour réaliser la tâche que nous lui demandons, c'est à lui à se débrouiller pour trouver la meilleure solution. Cette méthode d'apprentissage est aujourd'hui considérée comme étant la meilleure manière de stimuler la créativité des machines car une IA est capable d'effectuer des milliers de tentatives en simultané, contrairement à un être humain (Brenet, 2024).

4.4.3. Réseaux de neurones (Neural Networks)

Le concept de réseaux de neurones est un concept clé du Machine Learning. Ce sont des modèles inspirés du fonctionnement du cerveau humain car ils fonctionnent de la même manière. Un réseau de neurones artificiels est composé de neurones artificiels qui sont conçus pour se parler les uns les autres avec pour objectif d'apprendre. Chaque neurone va intercepter des informations et les transformer pour ensuite les envoyer aux autres neurones. Les réseaux de neurones sont considérés comme une forme d'apprentissage automatique. Les réseaux neuronaux sont également extrêmement rapides dans l'exécution de calculs, les rendant parfaitement adaptés au traitement de quantités d'informations colossales en un temps record (Brenet, 2024).

Pour ce qui est du fonctionnement de ces réseaux neuronaux, il est en réalité assez simple. Les neurones reçoivent des données d'entrée et chaque neurone effectuera des calculs avant de transmettre le résultat aux autres neurones. Les connexions entre les neurones ont un certain poids et sont autrement dit pondérées. Cela veut dire que certaines connexions « pèsent » plus que d'autres et c'est ce poids qui permet au réseau de neurones de reconnaître des schémas et faire des prédictions (Brenet, 2024).

Les réseaux neuronaux sont composés de plusieurs couches. La première couche est la couche recevant les données d'entrée, telles que du texte, des images ou d'autres types de données. Les couches intermédiaires, autrement appelées les couches cachées, ont pour objectif d'effectuer des calculs complexes afin d'extraire les caractéristiques importantes des données reçues par la première couche. La dernière couche est appelée la couche de sortie et c'est elle qui est responsable de la production du résultat final du réseau (Brenet, 2024).

La figure ci-dessous représente un réseau de neurones simple, composés de peu de couches. Cela correspond au Machine Learning. Ce réseau de neurones simple est mis en parallèle avec un réseau de neurones profond, composé de beaucoup plus de couches et représentant le Deep Learning, développé juste après.

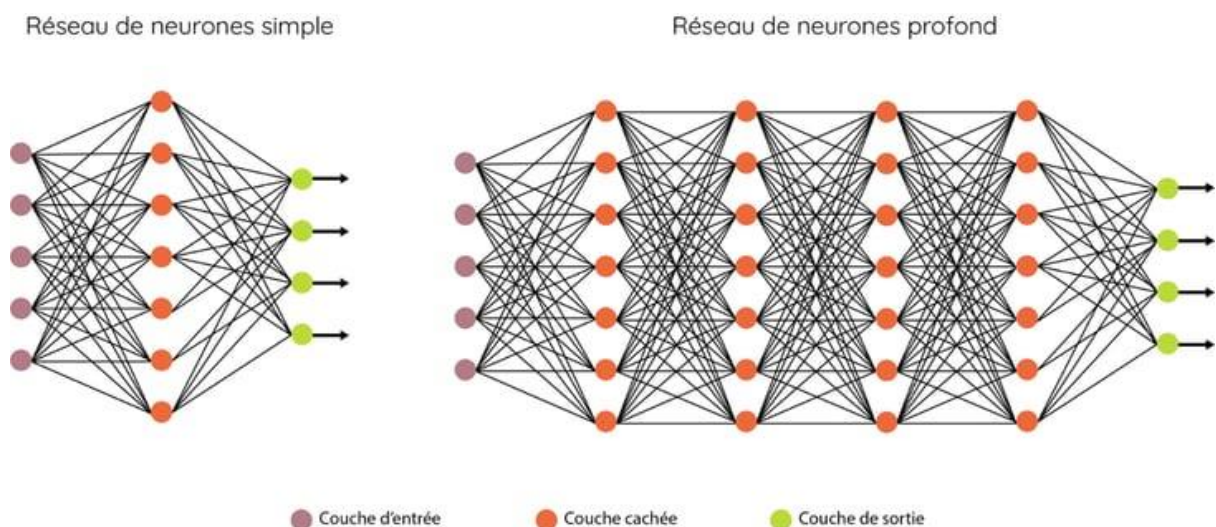


Figure 11 : Illustration d'un réseau de neurones simple et d'un réseau de neurones profond

Source : Yol, A., (2021). *La différence entre IA, Deep Learning, Machine Learning en agriculture*. Dilepix. Consulté le 13 avril 2025 à l'adresse <https://www.dilepix.com/blog/difference-intelligence-artificielle-deep-learning-agriculture>

4.4.4. Deep Learning (DL)

Le Deep Learning (apprentissage profond) est une branche du Machine Learning développé ci-dessus et dont l'objectif final est de résoudre des problèmes complexes. Il est basé sur des réseaux de neurones artificiels (Artificial Neural Network, ANN). Il utilise des réseaux de neurones dits « profonds », c'est-à-dire des réseaux capables d'apprendre mais également d'apprendre à apprendre. Il est capable de dégager des données complexes, des schémas hiérarchiques et des caractéristiques dans les données (Brenet, 2024).

Dans le cas du Deep Learning, on se passe de l'étape de détermination des variables qui caractérisent de phénomène étudié et ce, grâce au réseau de neurones artificiels développés.

Le DL est de plus en plus performant grâce à la puissance de calcul disponible (ordinateurs de plus en plus puissants), mais également avec l'amélioration des algorithmes et le volume croissant de données disponibles. Le nombre de couches de neurones augmente également drastiquement, comptant aujourd'hui pas moins d'une centaine de couches et des millions de neurones (Ejzyn, 2024).

4.4.5. *Natural Language Processing (NLP)*

Le Natural Language Processing n'est ni plus ni moins que la capacité d'un système à comprendre et à manipuler le langage humain. Durant les 10 dernières années, l'utilisation de réseaux de neurones profonds a révolutionné le Natural Language Processing car les modèles d'analyse du langage naturel basés sur le Deep Learning ont permis des améliorations significatives dans de nombreuses missions telles que la traduction, l'analyse de sentiments ou encore la génération de texte (Brenet, 2024).

Comme le démontre le schéma ci-dessous, les deux tâches principales du NLP sont la compréhension du langage naturel (Natural Language Understanding, NLU) et la génération de langage naturel (Natural Language Generation, NLG) (Brenet, 2024).

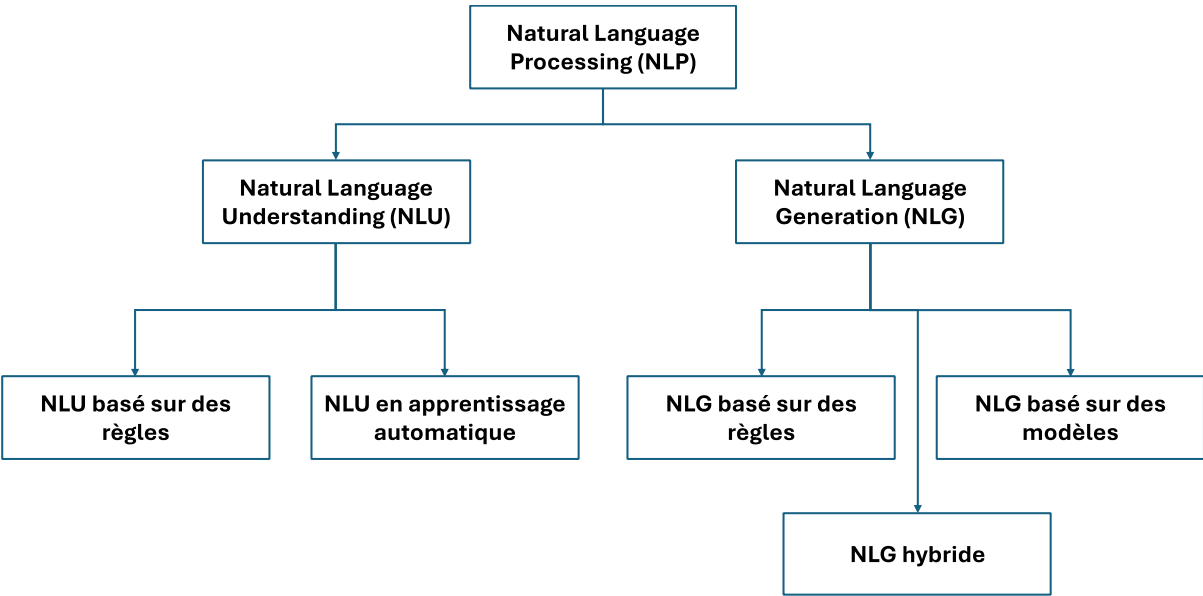


Figure 12 : Tâches du Natural Language Processing (Brenet, 2024).

La compréhension du langage naturel consiste en la capacité d'une machine à déchiffrer le sens caché d'un texte ou d'une conversation, c'est-à-dire aller bien au-delà d'une simple traduction et il existe pour ce faire deux méthodes. La première méthode, **basée sur les règles**, se distingue par des modèles linguistiques prédéfinis pour interpréter du texte. Ceux-ci sont souvent des systèmes experts pour une seule tâche. La deuxième méthode, **basée sur l'apprentissage automatique**, utilise par exemple des réseaux de neurones afin d'entraîner des algorithmes pour comprendre et interpréter le langage naturel en utilisant des données d'entraînement. Ces modèles sont pour cette raison capables de s'adapter à de nombreuses tâches (Brenet, 2024).

La génération de langage naturel fait référence à la capacité à produire du texte ou une conversation correcte, tant sur le plan grammatical que de la richesse sémantique, dans le but de créer une conversation fluide et intelligible. La génération de langage naturel se base sur des algorithmes d'apprentissage automatique et qui utilisent des données structurées telles que des bases de données, des statistiques, etc. afin de générer un texte cohérent (Brenet, 2024).

Il existe trois formes de génération de langage naturel. La première est **basée sur des modèles** de langage pré-entraînés pour générer du texte tel que le fait GPT-4 par exemple. Ce sont des modèles adaptés à des tâches spécifiques. La deuxième forme se **base sur des règles** linguistiques pour générer du texte. Ces règles peuvent être programmées manuellement ce qui permet une maîtrise du contenu généré. La dernière forme est une forme **hybride** des deux précédentes, permettant des résultats plus précis (Brenet, 2024).

4.5. Applications de l'IA

Les applications de l'intelligence artificielle sont de plus en plus nombreuses et il serait d'ailleurs impossible de toutes les lister compte tenu de l'évolution extrêmement rapide de cette technologie. Ce point n'est donc pas une liste exhaustive de toutes les applications de l'IA mais bien un extrait de celles qui pourraient le plus impacter notre vie quotidienne.

Un premier secteur qui a déjà été transformé par l'intelligence artificielle est le secteur de la santé. Elle a amélioré considérablement les diagnostics et les prestations de soins grâce à sa faculté d'analyse de quantité de données astronomique et sa capacité de s'adapter à chacun des patients. L'IA permet d'améliorer de manière significative les diagnostics médicaux mais elle est également une aide précieuse dans la recherche. Elle est capable de prendre des décisions en tenant compte d'un grand nombre de facteurs, dépendants du patient, afin de lui fournir les soins les plus adéquats. Les algorithmes de l'IA font d'elle un outil indispensable dans l'analyse et la recherche grâce à sa rapidité d'exécution. L'IA a également fait ses preuves en oncologie, démontrant sa capacité à détecter des cancers bien avant qu'ils ne soient visibles à l'œil nu (Brenet, 2024).

Un autre secteur fortement impacté par l'intelligence artificielle est le secteur automobile et plus précisément les voitures à conduite autonome. Cela fait déjà de nombreuses années que l'implémentation de l'IA dans le secteur automobile occupe les développeurs et chercheurs et son utilisation dans nos voitures modernes se démocratise de plus en plus. Il n'existe aujourd'hui pas moins de 5 niveaux d'autonomie allant de la simple aide à la conduite au niveau d'autonomie totale mais ceci n'est pas encore autorisé en Europe. L'IA permet de recréer en laboratoire des environnements virtuels pour améliorer les algorithmes. L'idée d'intégrer l'IA dans nos voitures peut être prometteuse sachant que 90% des accidents de voiture dans le monde sont dus à des erreurs humaines, bien que certaines personnes restent craintives de perdre le contrôle sur certains aspects (Brenet, 2024).

Les « chatbots » et assistants virtuels ont également largement contribué à l'amélioration de l'expérience de l'utilisateur en simplifiant les interactions et en fournissant des réponses instantanées. Les « chatbots » alimentés par l'IA sont des systèmes qui sont capables de simuler des conversations humaines et ne se contentent pas de simplement répondre aux questions mais également d'orienter les utilisateurs lors des interactions. Les « chatbots » s'améliorent en permanence et ont l'avantage d'être disponibles 24 heures sur 24 et sept jours sur sept. Ils permettent de réduire la charge de travail du personnel afin de leur laisser plus de temps pour des tâches à plus grande valeur ajoutée (Brenet, 2024).

De manière générale, nous pouvons constater que l'intelligence artificielle a déjà de nombreuses applications aujourd'hui et que son nombre d'applications ne cessera de croître avec l'amélioration de l'IA. Elle permet un gain de temps, tant pour les entreprises que pour les utilisateurs, mais permet également de réduire les risques, d'améliorer les contrôles et bien d'autres choses.

4.6. Limites, biais et éthique

Bien que l'intelligence artificielle suscite un grand enthousiasme de la part de ses utilisateurs, et ce, dans de nombreux domaines, l'IA est pour autant loin d'être parfaite. Elle présente des limites techniques, des risques de biais mais fait également apparaître des enjeux éthiques majeurs.

La principale limite technique liée à l'IA est en réalité en grande partie due à l'homme. En effet, l'intervention de l'homme est nécessaire pour définir, tester, valider et maintenir une IA car les données fournies pour la nourrir doivent être sélectionnées et préparées afin qu'elles puissent être utilisées pour l'entraîner. Cette extraction de données est extrêmement coûteuse en temps (Hours, 2019).

Une autre limite est le fait que les ordinateurs et bases de données nécessaires pour faire fonctionner une IA doivent être en marche de jour comme de nuit sans interruption. Ceci représente par conséquent un coût énergétique considérable pour les entreprises possédant de tels outils. A cela s'ajoute également la dimension durable, car en effet, maintenir en permanence ces ordinateurs en marche pollue énormément. L'Agence internationale de l'énergie a estimé qu'en 2023, l'intelligence artificielle représentait 1,5% de la consommation électrique mondiale. Cette part d'énergie risque de croître encore compte tenu de l'ampleur que prend l'IA dans la vie de tous les jours (Institut Supérieur de l'Environnement (ISE), 2024).

D'autres limites telles que la difficulté de comprendre de l'humour, des figures de style ou encore du sarcasme font que l'IA est encore loin d'être parfaite. S'ajoutent à cela le fait que l'IA n'est pas capable de comprendre le contexte de ce qu'elle fait, qu'elle n'est pas capable de hiérarchiser des alertes ou encore d'intégrer des émotions. L'IA a donc encore une belle marge de progression (Ejzyn, 2024).

Un biais peut se manifester lorsqu'elle reproduit ou amplifie des préjugés présents dans les données d'entraînement. Les données utilisées pour entraîner les modèles peuvent involontairement contenir des biais dus à des préjugés humains. Ces biais peuvent avoir des conséquences considérables. Par exemple, une IA développée pour analyser des CV dans un processus de recrutement automatisé peut comporter des biais liés au genre ou à la race, entraînant une discrimination à l'encontre de certains candidats. Afin d'atténuer ces biais, il faut apporter des ajustements au modèle dans le but de réduire au minimum les préjugés et ceci est de la responsabilité des concepteurs de s'assurer que le nombre de biais soit le plus faible possible. Un biais intrinsèque à l'IA est le fait qu'elle fonctionne comme une boîte noire. Une IA est incapable d'expliquer comment elle raisonne pour arriver à un résultat. Ce manque de transparence peut rendre compliqué l'évaluation de la fiabilité de ses décisions (Brenet, 2024).

Finalement, il est important de traiter l'aspect éthique des intelligences artificielles. En effet, ces dernières utilisent des grandes quantités de données et celles-ci sont parfois des données personnelles identifiables, c'est-à-dire qu'elles permettent d'identifier clairement une personne. Nous sommes donc en droit de nous demander ce qui est fait de ces données après utilisation et si celles-ci sont réellement en sécurité (Brenet, 2024).

Il faut finalement mentionner le fait que l'essor de l'IA pourrait dans un futur plus ou moins proche remplacer des êtres humains dans la réalisation de certaines tâches répétitives, causant aujourd'hui déjà, une inquiétude sociale. L'IA transformera incontestablement le marché de l'emploi rendant certains postes obsolètes (Brenet, 2024).

L'IA est un outil très puissant mais peut s'avérer dangereux dans les mains de mauvaises personnes. Il en va de notre responsabilité à tous de s'informer sur cette technologie et de l'utiliser à bon escient. L'IA fera incontestablement partie de nos vies, si ce n'est déjà le cas, et il est évident que l'État et les différentes autorités ont un rôle clé à jouer pour instaurer des règles et des limites avant qu'il ne soit trop tard. L'IA est une technologie en plein essor mais qui nécessite clairement des ajustements, tant sur le niveau technique, que de l'éthique et il existe de nombreux autres défis liés à l'IA que ceux cités dans ce dernier point.

Partie III – Question de recherche

1. Question de recherche

Comme nous avons pu le constater dans l'introduction générale, mais également dans la définition des différents concepts, l'environnement dans lequel évoluent les entreprises est de plus en plus incertain et les évolutions engendrent de nouveaux risques et zones d'incertitudes.

Le secteur industriel est un secteur essentiel à notre économie qui a subi de nombreux changements au cours des derniers siècles. Ces changements sont liés à des avancées technologiques. Les quatre révolutions industrielles que nous avons vécues jusqu'à présent ont permis des gains en efficacité, en efficience, élargissant au passage le champ des possibilités. Ces changements ont également modifié l'environnement dans lequel évoluent les entreprises et tous les acteurs économiques en général. D'autres événements exogènes, plus récents, tels que les guerres et la crise sanitaire du Covid-19 ont exercé une importante influence sur le secteur industriel.

Nous avons vu que la gestion des risques était primordiale au bon fonctionnement d'une entreprise et qu'il existe une multitude de risques, liés à l'activité économique ou non, et que chaque entreprise a un univers de risques qui lui est propre. La gestion des risques dépendra donc des risques identifiés par l'entreprise, mais également du rapport que l'entité a par rapport à ces risques. Nous avons également identifié des limites à la gestion des risques, pouvant dans certains cas restreindre son efficacité.

De la même manière que pour la gestion des risques, nous avons déterminé que le contrôle interne était crucial dans le but de fournir une assurance raisonnable quant à la possibilité de réaliser les objectifs de l'entreprise. Ce contrôle interne est fortement recommandé pour toutes les entreprises mais est obligatoire pour certaines entités telles que les entités d'intérêt public ou encore les pouvoirs locaux belges. Ici encore, il existe des limites au contrôle interne, pouvant restreindre son efficacité.

Finalement, le sujet de l'intelligence artificielle a été largement développé, en démontrant sa croissance rapide et ses nombreuses applications dans des secteurs divers et variés. Sa capacité à apprendre par elle-même sur base de données d'entraînement rend cette technologie prometteuse pour tous les secteurs y compris le secteur industriel.

Au vu des concepts développés ci-dessus et des limites identifiées pour chacun d'eux, il semblait intéressant de se focaliser davantage sur les applications de l'intelligence artificielle dans la gestion des risques et le contrôle interne. Pour ces raisons, la question de recherche suivante a été formulée :

« Quel est le degré d'implémentation de l'Intelligence Artificielle (IA) dans la gestion des risques et le contrôle interne des entreprises industrielles ? »

2. Hypothèses

En vue d'apporter une réponse à la question de recherche traitant du degré d'adoption de l'intelligence artificielle dans la gestion des risques et le contrôle interne dans les entreprises industrielles, il est pertinent de formuler des hypothèses permettant de guider l'analyse qui suivra. Ces hypothèses se basent sur des constats issus d'une première revue littéraire, mais également sur des éléments contextuels du secteur industriel, ainsi que sur les limites de la gestion des risques et du contrôle interne.

2.1. Hypothèse 1

Une première hypothèse que nous pouvons émettre est que le degré d'adoption de l'intelligence artificielle dans la gestion des risques ainsi que dans le contrôle interne des entreprises industrielles est, à l'heure actuelle, faible, compte tenu des limites liées aux contraintes technologiques et financières liées tant au secteur industriel, qu'à l'IA elle-même. Nous avons vu dans le chapitre dédié à l'IA que la mise en place d'un tel système peut être très coûteux car il nécessite des quantités de données considérables ainsi que des systèmes de calculs capables de traiter les données. D'autres raisons pourraient évidemment expliquer cela.

2.2. Hypothèse 2

Une autre hypothèse que nous pourrions formuler est le fait que les grandes entreprises et groupes industriels ont un degré d'adoption supérieur aux petites entités, ceci pouvant être expliqué notamment par la différence des ressources disponibles. Ici à nouveau, le coût de la mise en place d'un tel système pourrait expliquer cette divergence entre les plus grandes entités et les plus petites.

2.3. Hypothèse 3

Nous pouvons également avancer l'hypothèse, qu'actuellement, l'intelligence artificielle est davantage utilisée dans l'identification et l'évaluation des risques, ainsi que dans les activités de contrôle et de détection d'anomalies. L'IA serait, au contraire, moins utilisée pour la prévention et l'élaboration de solutions.

Ces hypothèses seront confrontées à une revue de la littérature ainsi qu'à une enquête auprès d'entreprises industrielles, afin de pouvoir les confirmer ou non, tant sur le plan théorique que pratique. Cette étude permettra de mieux comprendre le niveau réel d'intégration de l'IA dans la gestion des risques et du contrôle interne dans les entreprises industrielles, mais également de comprendre les raisons du niveau d'adoption actuel de l'IA.

Partie IV – Revue spécifique de la littérature

1. Objectifs de l'étude

L'objectif de cette revue littéraire est d'apporter une base théorique solide permettant d'évaluer le degré d'adoption de l'intelligence artificielle dans la gestion des risques et du contrôle interne des entreprises industrielles. Cette étude se basera tant sur des aspects théoriques pouvant expliquer le degré d'adoption actuel, que sur des études de cas réalisées, permettant un premier recensement. L'objectif sera de confronter différentes sources afin de pouvoir formuler une réponse objective à la question de recherche. Cette première réponse sera confrontée plus tard dans ce travail à une analyse empirique, permettant de la mettre en perspective par rapport au secteur industriel belge. L'objectif ultime est évidemment de pouvoir confirmer ou non les hypothèses développées ci-dessus.

Dans un premier temps, nous étudierons les différents facteurs pouvant influencer le degré d'adoption de l'intelligence artificielle, tant dans la gestion des risques que le contrôle interne. Ceci permettra de poser des bases solides, nécessaires à la compréhension de la suite de l'étude. Par la suite, nous étudierons l'adoption de l'intelligence artificielle dans la gestion des risques et du contrôle interne en développant les applications de l'IA dans ces domaines. Nous traiterons également des avantages et des limites de l'IA et feront un rapport de l'état actuel de son adoption dans le secteur industriel, ainsi qu'une comparaison avec les autres secteurs. Nous terminerons cette revue littéraire par une conclusion intermédiaire qui servira de base pour une analyse comparative avec l'étude empirique développée plus tard dans ce travail.

Afin de garantir une compréhension approfondie et équilibrée des thématiques abordées, cette étude se basera à la fois sur des publications d'entreprises expertes dans le domaine telles que Deloitte, McKinsey, KPMG, PwC ou encore EY, mais également sur des sources académiques reconnues. Les sources académiques permettent un cadre théorique rigoureux et validé par la recherche, là où les rapports des entreprises expertes se basent sur l'observation directe des pratiques d'entreprises. La combinaison de ces deux sources offre une approche enrichie et pertinente, nécessaire pour appréhender de façon objective l'adoption de l'IA dans la gestion des risques et du contrôle interne dans le secteur industriel.

2. Technology Acceptance Model (TAM)

Quand il est question d'étudier le degré d'implémentation de l'IA dans le contrôle interne et la gestion des risques, il peut être opportun de comprendre comment et pourquoi les entreprises, adoptent ou non, l'intelligence artificielle afin de les assister dans la réalisation de ces tâches. Pour ce faire, un modèle a été développé à la fin des années 80 par Fred Davis, nommé le Technology Acceptance Model ou Modèle d'Acceptation des Technologies en français (Baudet & Lebraty, 2018).

Ce modèle évoque le fait que l'acceptation d'une nouvelle technologie au sein d'une entreprise se base sur deux facteurs fondamentaux que sont l'utilité perçue (Perceived Usefulness, PU) et la facilité d'utilisation perçue (Perceived Ease of Use PEOU). L'utilité perçue fait référence à la manière dont l'utilité est perçue par ses utilisateurs et à quel point cette nouvelle technologie peut améliorer les performances au travail. La facilité d'utilisation, quant à elle, fait référence aux croyances des utilisateurs quant aux efforts qu'ils devront fournir pour utiliser ce nouveau système. Ce modèle se base donc sur la perception qu'ont les utilisateurs de la nouvelle technologie et non d'un retour sur expérience. Ce modèle permet donc de souligner les facteurs influençant l'adoption de nouvelles technologies et dans le cas de ce travail, de l'intelligence artificielle (Baudet & Lebraty, 2018).

Le schéma ci-dessous est une représentation du TAM.

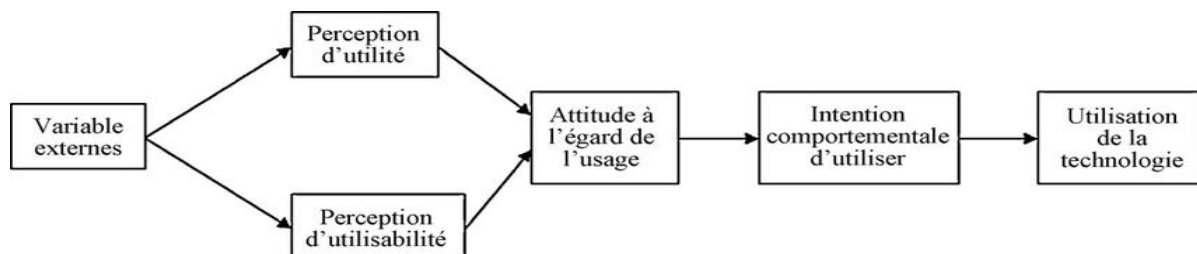


Figure 13 : Modèle d'acceptation de la technologie

Source : SI & Management. (s.d.). TAM, *Modèle d'acceptation des technologies: difficultés et avantages perçus* – F. Davis. Consulté le 6 mai 2025 à l'adresse <http://www.sietmanagement.fr/tam-modele-dacceptation-des-technologies-difficultes-percues-et-avantages-percus-f-davis/>

Le modèle établi par Davis se base sur les trois hypothèses suivantes :

- La facilité d'utilisation perçue par un utilisateur influence de manière positive son utilité
- Les deux variables influencent de manière directe l'attitude de l'utilisateur envers le système
- Cette attitude influence par la suite l'intention d'utiliser cette technologie

(Baudet & Lebraty, 2018)

Ce modèle a été construit sur base de deux études empiriques, d'une part une expérimentation en laboratoire avec 112 utilisateurs, et d'autre part un questionnaire administré auprès de 40 utilisateurs. De ces deux études est ressorti que l'utilité perçue par les utilisateurs a une forte corrélation positive avec l'intention d'utilisation de la nouvelle technologie, et que cette corrélation est plus forte qu'avec la facilité d'utilisation. Il en sort également que la facilité

d'utilisation influence de manière indirecte l'intention d'utilisation à travers l'utilité perçue (Baudet & Lebarty, 2018).

Dans le cas de l'implémentation de l'intelligence artificielle dans la gestion des risques, il s'agit donc de voir si l'IA est perçue comme ayant une utilité suffisante dans le cycle de gestion des risques (cf. Partie II, Chapitre 2) mais également de voir si l'IA est perçue par les équipes responsables comme étant facile d'utilisation. De la même manière, l'IA doit être perçue comme utile et facile d'utilisation si elle est implémentée dans le contrôle interne, en étant par exemple intégrée dans le COSO (cf. Partie II, Chapitre 3). En somme, l'IA doit améliorer l'efficacité de ces processus sans pour autant davantage complexifier ses processus. Chaque entreprise aura une perception différente, dépendant de facteurs développés dans le point suivant.

Nous pouvons donc conclure que la perception par les utilisateurs de l'utilité et la facilité perçue de l'usage d'une nouvelle technologie constituent des facteurs pouvant influencer le degré d'implémentation de l'IA dans le contrôle interne et la gestion des risques.

3. Facteurs influençant l'adoption de l'IA

3.1. Facteurs organisationnels et humains

L'implémentation de l'intelligence artificielle dans la gestion des risques et le contrôle interne dépend fortement des facteurs organisationnels et humains qui conditionnent son implémentation, mais également son efficacité et sa pérennité. Ce sont, dans notre cas, des facteurs qui déterminent la capacité d'une entreprise à intégrer l'IA dans son cycle de gestion des risques et son contrôle interne.

Un premier facteur à relever dans le cadre de l'implémentation de l'IA au sein d'une entreprise, c'est sa gouvernance. Celle-ci doit être claire et comprise par tout le monde mais elle doit également être alignée avec une certaine stratégie numérique. En effet, une étude réalisée par AuditBoard démontre qu'un excès de confiance et un manque de compréhension de l'IA peut engendrer de lourdes conséquences pour l'entreprise. Il faut donc définir de manière précise l'utilité de l'IA dans la tâche en question, la manière dont il faut l'utiliser et gérer les données, mais il faut également former les employés à son utilisation et définir les limites de celle-ci. Il faut donc comprendre et maîtriser l'IA avant de l'implémenter (AuditBoard, 2024).

Il est également important de prendre en considération la maturité numérique de l'entreprise. Dans un rapport publié par Deloitte en 2025, leur étude démontre que la vitesse à laquelle les technologies évoluent ne représente pas la vitesse à laquelle les entreprises adoptent ces nouvelles technologies. En effet, peu importe à quel point les technologies évoluent ou à quel point les développeurs d'IA poussent à leur utilisation, leur adoption sera toujours limitée par les capacités de l'entreprise souhaitant mettre en place cette nouvelle technologie (Rowan et al., 2025).

De plus, nous l'avons abordé dans la partie dédiée à l'intelligence artificielle, le développement d'une IA nécessite des quantités de données considérables. L'entreprise doit donc être en mesure de collecter et d'intégrer toutes ces données afin de les utiliser de manière efficace pour l'entraînement de leur IA. L'accès à une information qualitative mais également quantitative peut être un facteur limitant, ou au contraire catalyseur, afin d'implémenter une IA efficace tant dans la gestion des risques que le contrôle interne.

A cela s'ajoute le fait que l'entreprise doit disposer des compétences pour mettre en place une IA efficace ainsi que sa maintenance. Le défi est ici de combiner deux domaines, à savoir l'IA et la gestion. Comme mentionné dans un rapport publié par Supervizor, il est nécessaire de former ses employés à ces nouvelles technologies à travers des formations par exemple. Il est d'ailleurs mentionné dans ce rapport qu'il faut considérer l'IA comme un assistant et non comme un remplaçant. Il est donc primordial que les employés maîtrisent l'IA mise en place afin de pouvoir libérer du temps pour des tâches qu'elle n'est pas capable de réaliser (Supervizor, 2025).

La connaissance et la compréhension de l'IA sont également primordiales pour assurer un bon fonctionnement de l'IA au sein de l'entreprise. Cette compréhension leur permet d'identifier les points d'attention ainsi que d'identifier les informations clés de manière plus efficace. Il est donc important que les employés utilisant de l'IA dans leurs tâches développent des compétences interdisciplinaires. Ces compétences sont par exemple la compréhension et de l'utilisation d'outils statistiques nécessaires à la gestion de données (Jöhnk et al., 2020).

Finalement, l'implémentation de l'IA dans le contrôle interne et la gestion des risques doit être cohérente avec la stratégie de l'entreprise. Dans un rapport publié par Deloitte en 2023, l'importance d'un équilibre entre les capacités technologiques et une gestion prudente est soulignée. Il est essentiel d'adopter l'IA, non pas pour le simple fait de l'appliquer, mais bien parce qu'elle constitue un réel levier pour l'entreprise (Cabanis Dib Garrido, 2023).

3.2. Facteurs financiers

Nous avons vu dans la partie dédiée à l'intelligence artificielle que l'implémentation d'une telle technologie pouvait s'avérer très coûteuse. Ce coût est notamment lié au fait qu'il faut développer ou acheter le système, mais également disposer d'une infrastructure numérique suffisamment puissante afin que l'IA fonctionne de manière optimale. Il faut également prendre en compte la maintenance et la formation du personnel à son utilisation mais également la nécessité de récolte de données afin d'améliorer continuellement le système. Le coût d'implémentation et de fonctionnement peut varier de quelques dizaines de milliers d'euros à plusieurs millions d'euros, dépendant de la complexité et des applications qu'aura l'IA (Ta, 2024).

Le retour sur investissement (Return On Investment, ROI) est également un facteur important à prendre en considération lors de l'implémentation de l'IA dans la gestion des risques et le contrôle interne. Un article publié par Kellie Nuttall³ questionne ce retour sur investissements étant donné que le nombre d'investissements dans l'IA augmente. Le problème qu'elle a relevé dans son rapport est que le calcul du ROI est plus complexe que pour un simple investissement unique car dans le cas de l'IA, c'est un investissement qui s'ancre dans le business model de l'entreprise. Par conséquent, mesurer le ROI du projet pris isolément n'a pas de sens. Le ROI doit donc se baser sur des gains tangibles là où cela est possible, mais également sur des catalyseurs stratégiques tels que la vitesse, la résilience ou encore la différenciation. Le ROI doit guider l'implémentation de l'IA et non la limiter (Nuttall, 2025).

La part budgétaire que les entreprises souhaitent allouer à l'implémentation et à l'utilisation d'une IA dans leur gestion des risques et leur contrôle interne peut également influencer l'adoption ou non de cette technologie. Nous l'avons déjà mentionné, une IA peut représenter un coût considérable et il doit incontestablement être pris en compte lors de la budgétisation. Une étude⁴ réalisée par KPMG démontre que, en 2024, 86% des entreprises testent ou utilisent

³ Dr Kellie Nuttall est AI Institute Leader chez Deloitte Australia

⁴ Etude réalisée auprès de 1.800 entreprises actives dans six industries, réparties dans 10 pays.

déjà de l'intelligence artificielle et qu'ils estiment que d'ici 2027 ce nombre s'élèvera à plus de 99% (Odom, 2024). De cette même étude est ressorti que l'IA représentait, en 2024, 10% du budget IT des entreprises interrogées (KPMG, 2024). D'après une étude⁵ réalisée la même année par Deloitte, il est estimé que 78% des entreprises souhaitent augmenter leurs dépenses dans l'IA en 2025 (Rowan et al., 2025). McKinsey estime que dans les 3 prochaines années, 92% des entreprises souhaitent investir davantage dans l'IA et que seul 1% des entreprises actuelles considèrent avoir atteint une maturité sur le plan de l'IA (Mayer et al., 2025).

De cette même étude publiée par Deloitte, 11 facteurs pouvant entraver l'implémentation et le développement ont été analysés. L'un de ces facteurs représente « le manque d'engagement et/ou de financement de l'exécutif », où 19% des répondants considéraient cela comme une barrière au premier quadrimestre de l'année. Au quatrième quadrimestre de 2020, ce pourcentage a chuté à 14% (Rowan et al., 2025). Nous pouvons donc constater que la partie financement est un facteur déterminant de l'implémentation de l'IA, bien que cette tendance soit légèrement en baisse.

3.3. Facteurs légaux

Afin d'adopter l'intelligence artificielle de manière responsable et en se conformant aux règles en vigueur, il est intéressant de se pencher sur les principaux enjeux juridiques qui régissent cette technologie au sein des entreprises.

La première loi globale sur l'intelligence artificielle a été adoptée par l'Union Européenne en mars 2024. L'état du Colorado aux États-Unis a également adopté une loi similaire au mois de mai 2024 et d'autres lois semblables sont sur le point de voir le jour dans d'autres parties du monde (Shilling, 2025).

En Europe, c'est le *Règlement (UE) 2024/1689 du Parlement Européen du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) no 300/2008, (UE) no 167/2013, (UE) no 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle)*, qui régit l'utilisation de l'IA en général. Ce règlement porte également le nom de AI Act (Journal officiel de l'Union européenne).

L'objectif de ce règlement Européen est “d'améliorer le fonctionnement du marché intérieur et de promouvoir l'adoption d'une intelligence artificielle (IA) axée sur l'humain et digne de confiance, tout en garantissant un niveau élevé de protection de la santé, de la sécurité et des droits fondamentaux consacrés dans la Charte, notamment la démocratie, l'état de droit et la protection de l'environnement, contre les effets néfastes des systèmes d'IA dans l'Union, et en soutenant l'innovation.” (Règlement (UE) 2024/1689, Journal officiel de l'Union européenne).

⁵ Etude réalisée auprès de 2.773 entreprises réparties dans 14 pays.

Bien que tous les règlements ne soient pas identiques, ils reposent sur les trois mêmes fondamentaux : Les usages interdits, les usages limités et les usages fondamentaux (Shilling, 2025).

Les usages interdits font référence à des usages qui sont jugés comme étant trop risqués ou dangereux. Ceux-ci sont par exemple la manipulation de la prise de décision d'individus, portant préjudice à lui-même ou à d'autres individus. Ceci pourrait également être le fait de juger des personnes sur base de principes non fondés ou encore de surveiller des individus, violant ainsi leur intimité et vie privée. Les entreprises utilisant de l'IA dans leurs activités ont également l'interdiction formelle d'utiliser les informations récoltées pour d'autres fins que celles initialement prévues, en ce compris des activités discriminatoires, frauduleuses, diffamatoires ou encore de propagation de fausses informations, etc. (Shilling, 2025).

Les usages restreints sont des pratiques qui, bien qu'elles ne soient pas interdites explicitement, doivent être exécutées avec précaution. Ceci inclut par exemple l'identification biométrique, les processus d'embauche ou encore le traitement d'informations personnelles et confidentielles. Avant de traiter de telles données, les entreprises ont l'obligation d'effectuer une évaluation de l'impact de l'IA afin d'identifier les risques et l'utilité d'user de l'IA pour mener à bien leur tâche (Shilling, 2025).

Les usages fondamentaux de l'IA sont une réponse aux peurs qui ont émergé à la suite de la montée en puissance de cette technologie. Cinq fondamentaux doivent tous impérativement être respectés par les entreprises utilisant l'IA (Shilling, 2025).

Intégrité des données

Lors de l'entraînement de l'IA pour une mission précise, l'entreprise ne peut utiliser que des données précises, justes, légitimes, fiables et adaptées pour leur usage. Il est formellement interdit d'utiliser des informations discriminatoires, fausses, ou contenant des biais ou toute autre information pouvant générer de telles réponses (Shilling, 2025).

Transparence

Il est impératif que les entreprises utilisant l'IA informent les individus qui pourraient être impactés par l'utilisation de cette l'IA. Ces entreprises-là, même si le résultat n'est produit qu'en partie par une IA, ont l'obligation de mentionner aux individus concernés que de l'IA a été utilisée pour générer ce résultat (Shilling, 2025).

Contrôle humain

Avant d'utiliser les résultats produits par une IA, il est impératif que l'entreprise fasse revoir les résultats par un humain qualifié dans le domaine en question, afin de s'assurer de l'exactitude, de la légitimité et de la fiabilité des informations produites. Ces personnes doivent être formées pour reconnaître des informations incorrectes, biaisées ou discriminatoires (Shilling, 2025).

Tests et audits

Avant d'utiliser l'IA, il est impératif que l'entreprises teste son IA afin de s'assurer qu'elle fonctionne correctement et que les données utilisées lors de son entraînement, mais également

les résultats produits par l'IA, soient exempts de biais, d'erreurs, et utilisables pour l'objectif défini. Une fois l'IA testée et mise en place, l'entreprise doit procéder à des audits périodiques sur les nouvelles données utilisées pour entraîner l'IA, mais également sur les résultats qu'elle produit, afin de s'assurer que l'IA fonctionne toujours de manière optimale (Shilling, 2025).

Cybersécurité et vie privée

Les lois en matière de cybersécurité et de vie privée sont également d'application pour l'intelligence artificielle (Shilling, 2025). Ceci fait notamment référence au *Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE. (Règlement (UE) 2016/679, Journal officiel de l'Union européenne)*

3.4. Facteurs éthiques

L'implémentation de l'intelligence artificielle dans la gestion des risques et le contrôle interne, mais également dans une entreprise en général, s'accompagne d'enjeux éthiques pouvant influencer significativement sa décision d'adoption.

Une étude menée par Luciano Floridi et Josh Cowls, répartit en 5 groupes distincts les différents principes identifiés dans de nombreux autres rapports. L'objectif de ce rapport est de centraliser et de regrouper tous les principes éthiques concernant l'IA en un seul et même travail (Floridi & Cowls, 2019).

Bénéfice

L'intelligence artificielle doit bénéficier au plus grand nombre et prendre en compte le bien-être de tous. Ce principe prend également en considération l'aspect durabilité dans son ensemble. Lors de l'implémentation de l'IA dans une entreprise, il faut prendre en considération l'impact que celle-ci peut avoir sur l'environnement, tant celui de l'entreprise que l'environnement au sens écologique. En résumé, l'IA doit être bénéfique pour tout le monde (Floridi & Cowls, 2019).

Non-malveillance

Ce principe est complémentaire au précédent. En effet, il est demandé que l'IA fasse le plus de bien possible aux personnes concernées de près ou de loin par celle-ci, mais il est évident qu'elle ne peut être malveillante. Un point important de ce principe est le fait qu'il ne faut pas commettre d'infractions lors de l'utilisation d'informations à caractère personnel ou privé. Il faut opérer dans un cadre sécurisé afin d'éviter un usage abusif de celles-ci. Il est également important que les entreprises prennent leurs responsabilités en matière de gestion des risques relatifs à l'IA en trouvant des solutions. Aujourd'hui encore, il n'est pas clairement défini qui est responsable en cas de problème ; l'entreprise développant l'IA ou l'IA elle-même (Floridi & Cowls, 2019).

Autonomie

Nous entendons par autonomie le fait que l'être humain doit pouvoir garder son autonomie, malgré l'utilisation de l'IA. Lors du développement d'une IA, l'autonomie humaine doit être prise en considération. En d'autres termes l'IA ne peut pas nuire aux libertés humaines. Les humains doivent, à tout moment, être capables de décider ce qu'ils souhaitent faire eux-mêmes et ce qu'ils souhaitent déléguer à une IA. La liberté de l'IA doit donc être limitée et cette décision doit être révocable à tout moment (Floridi & Cowls, 2019).

Justice

Ce principe se base sur le fait que le développement d'une IA doit promouvoir la justice et éliminer tout type de discrimination. L'IA doit également être accessible de manière équitable à tout le monde. Ce principe reprend également le fait que l'IA doit être corrigée si dans le passé elle a commis des erreurs (Floridi & Cowls, 2019).

Explicabilité

Une IA est développée par quelques personnes qui sont spécialisées dans leur domaine mais l'objectif est que leur travail soit compris par tout le monde. Nous entendons par là le fait qu'il faut comprendre leurs motivations et les objectifs qu'ils souhaitent atteindre en l'implémentant dans l'entreprise. Il faut également être transparent et clair sur les effets de cette IA sur son environnement (Floridi & Cowls (2019).

4. L'Intelligence Artificielle dans le contrôle interne et la gestion des risques

4.1. Applications actuelles de l'IA dans le contrôle interne

Le contrôle interne peut aujourd'hui s'appuyer sur l'intelligence artificielle pour améliorer son efficacité. En effet, l'IA permet une précision accrue dans la détection de risques, elle permet d'élargir la couverture des contrôles, mais elle permet également une plus grande pertinence dans le ciblage des contrôles à effectuer. L'IA permet aussi d'automatiser certaines tâches telles que les procédures de conformité, les procédures internes et audits internes, mais également la vérification de transactions financières. L'IA permet également de réduire les erreurs humaines et le coût du processus de conformité. Ceci permet donc au département de contrôle de consacrer plus de temps à d'autres tâches telles que l'analyse et la compréhension des risques émergents ou encore la sensibilisation et l'accompagnement des opérateurs (Cabanis Dib Garrido et al., 2024).

Comme mentionné précédemment, l'intelligence artificielle est capable de traiter de grandes quantités d'informations. Cette capacité d'analyse peut être bénéfique pour limiter les risques de non-conformité car l'IA est capable d'analyser des textes réglementaires et en ressortir les modifications et les éventuels points d'amélioration à mettre en place par l'entreprise (Cabanis Dib Garrido et al., 2024).

Cette analyse de données permet également de relever des anomalies, des comportements suspects ou encore des fraudes ou erreurs avant même qu'elles ne surviennent ou aient un impact sur l'entreprise (Cabanis Dib Garrido et al., 2024). Dans un rapport publié par Ernst & Young en 2024, il est décrit que d'après leur expérience et les retours de leurs clients, L'IA a prouvé sa capacité à améliorer le processus de détection de fraudes (Bou Hamdan et al., 2024).

Dans une grande partie des fraudes, les malfaiteurs utilisent des identifiants factices, souvent créés uniquement dans le but de mener leurs activités frauduleuses. L'IA générative permet dans ces cas-là de détecter ce genre de manipulations, permettant ainsi de réduire les risques liés à ce type de fraudes (Bou Hamdan et al., 2024).

De plus, l'analyse massive de données permet de surveiller en permanence les opérations de l'entreprise afin d'identifier les signes d'un événement suspect ou tout simplement d'anticiper des risques avant qu'ils ne se produisent (Cabanis Dib Garrido et al., 2024). Cette analyse de données à grande échelle permet également à des IA génératives de produire des rapports et des synthèses sur base des données collectées, permettant ainsi un gain de temps considérable (Bou Hamdan et al., 2024).

L'utilisation de l'intelligence artificielle permet également de prioriser les alertes de surveillance des transactions dans le but d'optimiser l'allocation des ressources pour les investigations. Ceci est rendu possible grâce au « machine learning », développé précédemment, car cela permet de

classer les alertes en fonction de leur importance ou du risque qui leur est lié. L'adoption de l'IA permet de réduire de 15% les tâches manuelles, d'améliorer l'intégration des informations grâce notamment à des outils tels que des RPA⁶ afin de générer automatiquement des rapports, mais cela permet également d'améliorer la détection d'erreurs et de fraudes (Cabanis Dib Garrido et al., 2024).

Finalement, l'intégration de l'IA au contrôle interne offre une gestion dynamique du plan de contrôle permettant de générer une matrice de gestion des risques. Ceci est rendu possible grâce au Large Language Models, car ces modèles sont capables d'identifier des risques à partir de données que nous lui fournissons telles que le périmètre de l'audit ou encore le profil de l'entreprise. A partir de cela, des plans de contrôle peuvent automatiquement être générés, permettant de continuellement mettre à jour les matrices de contrôle sur base des évolutions réglementaires (Cabanis Dib Garrido et al., 2024).

4.2. Applications actuelles dans la gestion des risques

Avant de développer les applications de l'intelligence artificielle dans la gestion des risques des entreprises, il est important de revenir sur un concept important en gestion des risques, l'appétence au risque de l'entreprise. L'appétence au risque d'une entreprise correspond tout simplement aux risques qu'elle est prête à prendre. L'implémentation de l'IA peut causer de manière inhérente une augmentation ou une diminution de certains types de risques. Cela implique que l'appétence au risque pourrait nécessiter une révision pour certains types de risques (Bigham et al., 2018).

L'un des plus grands avantages d'implémenter l'IA dans la gestion des risques d'une entreprise est qu'elle leur permet de combler des failles dans leur système de gestion des risques, mais également d'améliorer leur résilience et de saisir les opportunités émergentes et de capitaliser dessus. Le fait d'utiliser de l'IA pour ce genre de tâches permet aux entreprises de consacrer plus de temps à des initiatives stratégiques, mais également de mitiger des risques émergents (Agarwal et al., 2024).

L'intelligence artificielle peut également contribuer à la diminution des risques auxquels une entreprise doit faire face. En effet, le « machine learning » permet de réaliser des prédictions plus précises et fiables quant à la probabilité qu'un risque se produise. Cela peut par exemple être utilisé pour mieux déterminer si un client payera dans les temps ou non (Boillet, 2018).

Une autre application de l'IA est la détection de fraudes. Le « machine learning » est capable d'identifier des fraudes grâce à un entraînement basé sur des données historiques. L'IA est capable d'identifier des comportements suspects, dans des transactions bancaires par exemple, mais également de faire un parallèle avec d'autres informations sur le comportement des

⁶ Robotic Process Automation: technologie permettant d'automatiser des processus répétitifs (UiPath, 2025).

personnes telles que l'analyse des courriels électroniques, l'analyse du calendrier ou encore les horaires de travail des employés (Boillet, 2018).

L'intelligence artificielle permet également à l'entreprise de s'adapter plus facilement et plus rapidement aux changements de son environnement mais également aux changements des réglementations. La capacité de ces systèmes à analyser de grandes quantités d'informations rend possible une analyse continue des réglementations, permettant à l'entreprise d'être mise au courant de manière automatisée d'éventuels changements dans ces réglementations (Agarwal et al., 2024).

L'IA permet également des meilleures prises de décisions dans les entreprises car, à travers des analyses quantitatives et qualitatives, les entreprises obtiennent une vision claire de leur univers de risques. Cette vision claire de leurs risques permet à l'entreprise de hiérarchiser les risques en fonction de leur probabilité et de leur impact et ainsi prioriser les risques les plus significatifs (Badman, 2024).

L'utilisation de l'IA dans la gestion des risques permet également d'assurer la continuité des activités. En effet, l'IA permet aux entreprises d'appréhender les risques en temps réel, afin d'y apporter une solution adéquate le plus rapidement et efficacement possible (Badman, 2024).

4.3. Limites de l'Intelligence Artificielle dans le contrôle interne et la gestion des risques

Nous avons vu ci-dessus que l'implémentation de l'intelligence artificielle dans le contrôle interne et la gestion des risques apportait de nombreux avantages tels qu'une meilleure efficacité dans l'analyse de données, mais également une meilleure identification d'erreurs ou de fraudes, un gain de temps, etc. Mais l'IA entraîne également avec elle des défis et comporte aussi des limites quant à sa contribution dans le contrôle interne et la gestion des risques.

Tout d'abord, l'IA est, comme nous l'avons déjà mentionné, dépendante des données d'entraînement utilisées. L'entreprise doit donc être en mesure de fournir des données de qualité car des mauvaises données pourraient engendrer des biais algorithmiques, rendant l'IA inexploitable (Cabanis, Dib Garrido et al., 2024).

Ensuite, une limite inhérente à l'utilisation d'une IA est le fait que l'investissement initial peut être assez conséquent et que ces systèmes nécessitent une infrastructure solide et une mise à jour constante. Comme nous l'avons mentionné dans les facteurs pouvant influencer l'implémentation d'une IA, le coût peut constituer un frein pour les entreprises quant à son implémentation (Cabanis Dib Garrido, et al., 2024).

Il est également important que l'entreprise définisse de manière claire une stratégie et des protocoles afin de gérer les aspects éthiques et réglementaires de l'utilisation de l'IA dans le cadre du contrôle interne et de la gestion des risques d'une entreprise (Cabanis Dib Garrido et al., 2024). Nous pouvons également constater cela dans les facteurs pouvant influencer l'implémentation de l'IA dans les entreprises, car il est primordial qu'elle soit consciente des

implications éthiques que peut avoir l'utilisation d'une IA et elle doit, par conséquent, prendre des mesures pour que l'impact éthique soit le plus positif possible.

De plus, nous avons pu constater dans les facteurs légaux pouvant influencer l'implémentation de l'IA, qu'un contrôle humain devait être effectué afin d'éviter des résultats biaisés ou discriminatoires. Le fait de devoir passer en revue les analyses faites par l'IA pourrait remettre en cause l'efficacité perçue par l'entreprise (Cabanis Dib Garrido et al., 2024).

L'IA n'a pas non plus de connaissance parfaite et approfondie de l'activité et ne connaît par conséquent pas les processus spécifiques à l'organisation dans tous ses détails. Chaque entreprise est différente et l'IA doit donc être adaptée à chacune d'entre elles. Sans connaissance parfaite de la structure de l'entreprise et de ses opérations, il peut s'avérer plus complexe d'identifier des sources de risques d'erreurs ou de fraudes par exemple (Supervizor, 2025).

L'IA ne possède également pas la capacité de faire des jugements nuancés tels que le ferait un être humain. Nous l'avons vu dans la partie dédiée au contrôle interne, il est nécessaire dans le d'apporter un jugement lors des investigations et c'est d'ailleurs pour cela que le contrôle interne fournit une assurance raisonnable et non une assurance totale. La gestion des risques est, comme nous l'avons vu précédemment, également dépendante d'un certain jugement humain et de l'appétence aux risques de l'entreprise (Supervizor, 2025).

Il est également important de prendre en considération le fait que l'IA n'apporte pas uniquement des aspects positifs. Bien qu'elle permette de détecter avec plus de facilité et plus de rigueur des fraudes, l'IA peut également en être la cause. La fraude existe depuis le début de l'humanité et l'évolution des outils qui sont à notre disposition font que les fraudeurs trouvent constamment des techniques plus efficaces pour commettre leurs « crimes », modifiant au passage les risques auxquels sont confrontés les entreprises (Jha, 2023).

Les possibilités offertes par l'intelligence artificielle sont nombreuses et permettent de progresser de manière multimodale en ciblant tant du texte que de la voix ou encore des vidéos. L'IA permet de rédiger des mails d'hameçonnage (phishing) de plus en plus réalistes et cela très rapidement. Ces mails sont réalisés de telle sorte qu'ils ne sont pas ou difficilement détectés par les mécanismes de contrôle des entreprises (Jha, 2023).

Le « Deepfake » correspond à des images ou des vidéos qui sont réalisées par une IA et qui peuvent mettre en scène des personnes dans des situations complètement fausses en reprenant leur apparence physique mais également leur voix et d'autres caractéristiques qui leur sont propres. Ces techniques peuvent être utilisées par des escrocs pour parvenir à leurs fins en faisant croire à leur victime que la personne avec qui ils conversent est une personne de confiance, voire une personne qu'ils connaissent personnellement. La Commission fédérale américaine du commerce a rapporté que des fausses vidéos d'Elon Musk pour escroquer des consommateurs auraient rapporté plus de deux millions de dollars américains en six mois (Jha, 2023).

Ce nouveau genre de risques nécessite donc d'adopter une nouvelle approche pour lutter contre la fraude. Il est désormais impératif de pouvoir les identifier avec certitude et de reconnaître que

ces menaces existent. Pour ce faire, des mesures peuvent être prises telles que la modification du modèle opérationnel de lutte contre la fraude en intégrant dans les contrôles la détection des « Deepfake ». Les entreprises doivent également assurer une évaluation continue et une analyse des risques liés aux « Deepfake » auxquels elle est confrontée. Finalement, les entreprises doivent réaliser des évaluations régulières des menaces afin de les comprendre, mais également pour identifier les vulnérabilités de l'entreprise afin de les corriger (Jha, 2023).

4.4. État actuel de l'adoption de l'Intelligence Artificielle dans le secteur industriel

Il est désormais intéressant de se pencher sur le degré d'adoption de l'intelligence artificielle au sein des entreprises à travers le monde. Pour ce faire, nous étudierons premièrement le degré d'adoption général de l'IA, tous secteurs et activités confondus. Nous nous pencherons ensuite sur le degré d'adoption de l'IA dans le secteur industriel uniquement et terminerons par le degré d'adoption de l'IA dans le contrôle interne et la gestion des risques des entreprises industrielles à travers le monde. Cette approche en entonnoir permettra de comprendre le contexte et l'importance du sujet.

4.4.1. Adoption globale de l'Intelligence Artificielle dans les entreprises

En 2021, IBM publie un rapport nommé « Global AI Adoption Index 2021 », qui, comme son nom l'indique, traite du degré d'adoption de l'intelligence artificielle dans les entreprises à travers le monde. Les données ont été récoltées auprès de 5.501 entreprises réparties en Chine (500), en France (500), en Allemagne (500), en Inde (500), en Italie (500), en Amérique Latine (1000), à Singapour (500), au Royaume Uni (500) et aux Etats-Unis (501) (IBM Watson, 2021).

De cette étude est ressorti que près de 33% des répondants ont affirmé déjà utiliser de l'IA dans leur entreprise, pourcentage quasiment identique à l'année 2020. Il en est également ressorti que près de la moitié des répondants explorent les possibilités qu'offre l'IA et que 43% des répondants ont accéléré l'implémentation de l'IA dans leur entreprise à la suite de la crise du Covid-19 bien qu'il ait également été souligné qu'il existait un certain manque de compétences en IA et que la complexification des données posait une difficulté supplémentaire (IBM Watson, 2021).

L'étude démontre également un degré d'adoption différent en fonction de la taille de l'entreprise. En effet, les plus grandes entreprises sont près de 70% plus susceptibles que les petites entreprises d'avoir déjà déployé l'IA dans leur organisation. 34% des répondants ont affirmé ne jamais avoir implémenté de l'IA dans un projet (IBM Watson, 2021).

Cette divergence du degré d'adoption en fonction de la taille de l'entreprise est également appuyée par une étude réalisée par KPMG en 2024. En effet, le graphique ci-dessous reprends la maturité de l'IA dans les entreprises en fonction de leur taille (basée sur le chiffre d'affaires). Nous constatons qu'entre 22% et 25% des entreprises sont considérées comme étant débutantes en matière d'IA, peu importe la taille de celles-ci. Néanmoins, nous pouvons constater une différence flagrante entre les entreprises ayant implémenté l'IA et les leaders en termes d'IA. En

effet, il existe une corrélation positive entre la taille de l'entreprise et le nombre d'entreprises ayant implémenté l'IA mais également le nombre d'entreprises leadeuses en termes d'IA (KPMG, 2024).

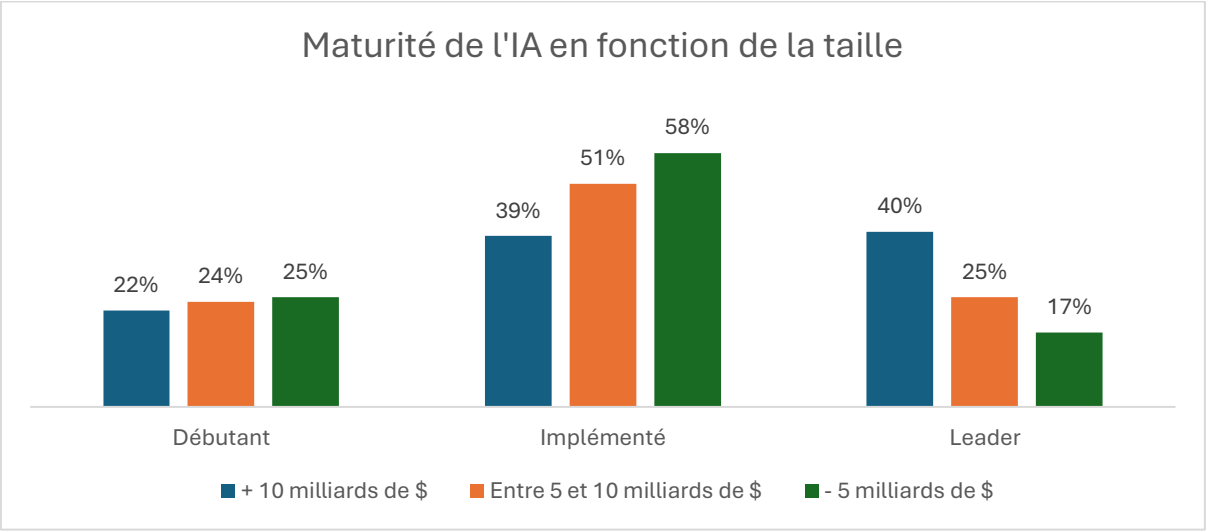


Figure 14 : Maturité de l'IA en fonction de la taille (KPMG, 2024).

Le graphique ci-dessous permet de visualiser où en sont les entreprises dans l'adoption de l'IA au sein de leur organisation.

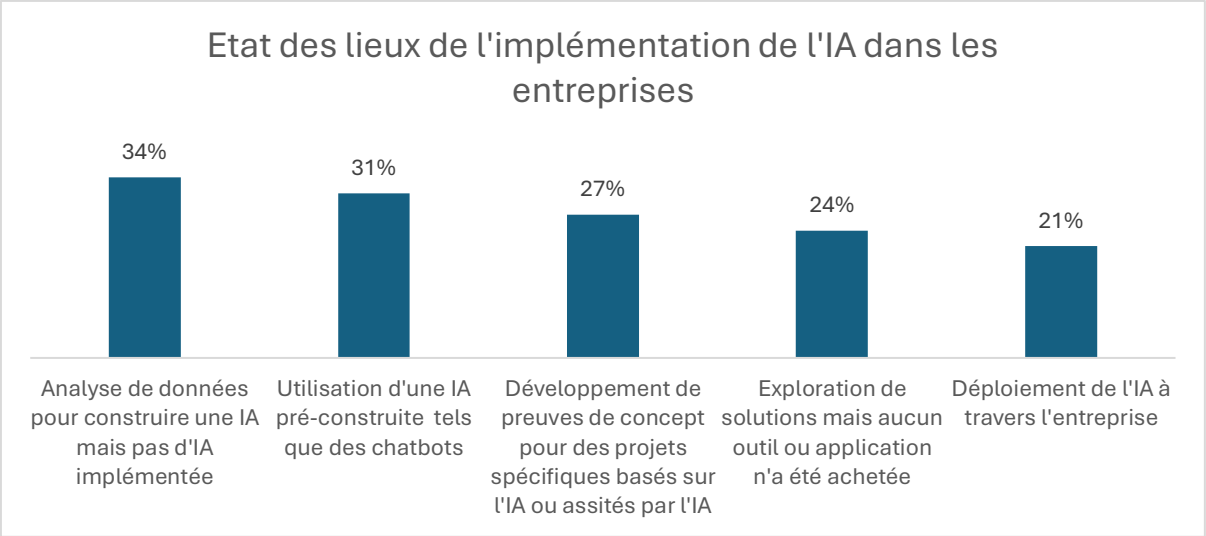


Figure 15 : État des lieux de l'implémentation de l'IA dans les entreprises (IBM Watson, 2021).

Une étude⁷ réalisée par Deloitte au quatrième trimestre de 2024 a été mise en parallèle avec une étude qu'ils avaient réalisé un an auparavant. La première étude avait démontré une certaine excitation quant à l'utilisation de l'intelligence artificielle dans les entreprises. Cette excitation s'est légèrement estompée au cours de l'année 2024 à la suite d'une certaine prise de conscience des potentiels impacts négatifs que son implémentation pourrait avoir. Il en ressort également que les résultats prometteurs des premiers projets de GenAI ont engendré une augmentation des investissements et des attentes dans la technologie (Rowan et al., 2025).

⁷ Etude réalisée auprès de 2.773 entreprises réparties dans 14 pays.

Le graphique suivant montre l'évolution du niveau d'intérêt de l'IA par rang entre le premier et le quatrième trimestre 2024 :

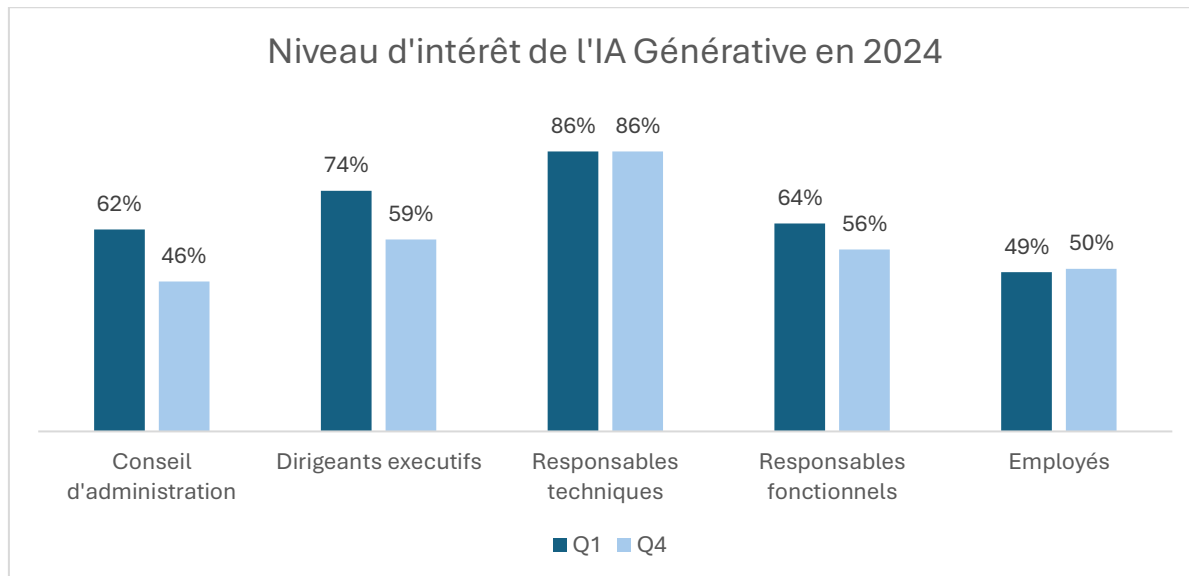


Figure 16 : Niveau d'intérêt de l'IA générative (Rowan et al., 2025).

Comme mentionné ci-dessus, le graphique démontre bien que l'intérêt pour l'IA générative a légèrement diminué, entre le premier et le quatrième trimestre, pour l'ensemble des rangs à l'exception des responsables techniques.

Cette même étude réalisée par Deloitte a également mis en avant le fait que 78% des répondants ont pour objectif d'augmenter leurs investissements dans l'intelligence artificielle pour l'année 2025. Il est également rapporté que plus de 66% des répondants estiment que moins de 30% de leurs essais actuels seront adoptés complètement dans les trois à six mois qui suivent, ce qui reflète le fait que les entreprises prennent le temps de faire des essais afin de voir ce qui correspond le mieux à leurs attentes (Rowan et al., 2025).

Finalement, il est intéressant de mentionner qu'il existe une différence dans le degré d'implémentation de l'intelligence artificielle en fonction du département de l'entreprise. D'après l'étude menée par Deloitte, nous pouvons constater que le département ou l'implantation de l'IA est la plus élevée est le département « IT », avec 28% des entreprises répondantes pour lesquelles c'est le cas. Au contraire le département « Legal, Risk, Compliance » est le département pour lequel seulement 1% des entreprises répondantes ont le plus implémenté l'IA (Rowan et al., 2025).

Une étude réalisée par BCG⁸ en 2024 démontre que seulement 26% des entreprises ont dépassé le stade de la preuve du concept et génèrent ainsi de la valeur. Sur 1.000 entreprises interrogées, seulement 4% d'entre elles ont développé des compétences en IA à la pointe du progrès et utilisent ces compétences pour générer de la valeur. 22% d'entre elles ont une stratégie intégrant de l'IA et ont développé des compétences leur permettant de commencer à créer de la valeur. Les 74% restants doivent encore faire leurs preuves en matière d'IA (de Bellefonds et al., 2024).

⁸ Boston Consulting Group

4.4.2. Adoption de l'Intelligence Artificielle dans les entreprises industrielles

Dans un rapport publié par BCG en 2024, une étude est réalisée concernant le degré d'adoption de l'IA dans le secteur biopharmaceutique, un sous-secteur du secteur industriel. Il y est mentionné que plus de la moitié de la valeur générée dans ce secteur est issue des ventes. Les entreprises de biopharmaceutiques utilisent l'IA générative pour la génération systématique de médicaments, de protéines et de processus biologiques. Elle permet également une personnalisation pour les patients et les prestataires de soins. L'IA permet de documenter les interactions et de cibler les patients grâce à leurs données médicales (de Bellefonds et al., 2024).

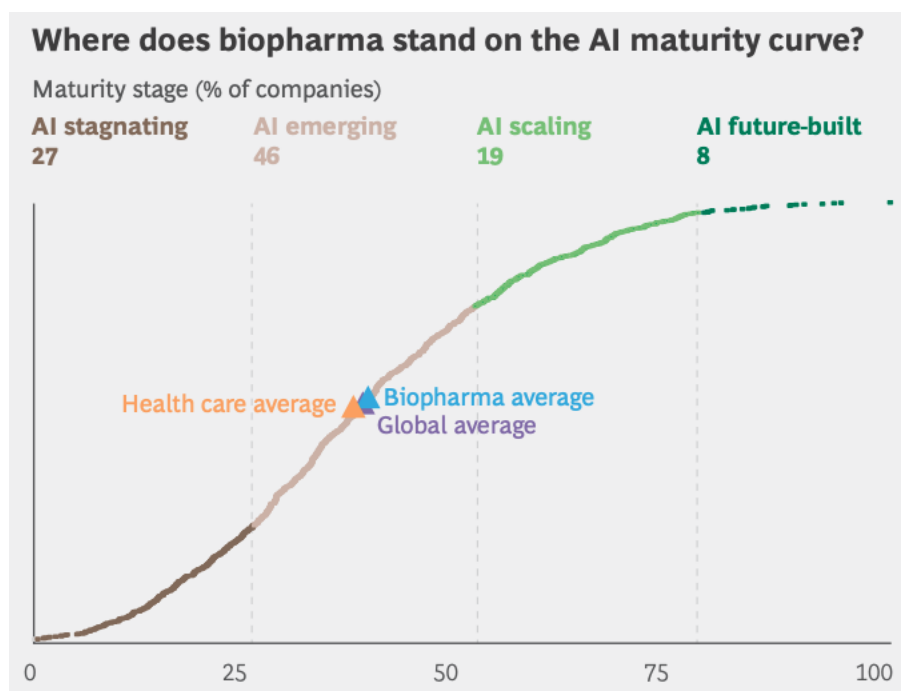


Figure 17: Where does biopharma stand on the AI maturity curve?

Source : de Bellefonds, N., Franke, M. R., Forth, P., Charanya, T., Apotheker, J., Grebe, M., Luther, A., Lukic, V., Nopp, C., de Laubier, R., Martin, M., & Sassine, J. (2024). Where's the Value in AI? Boston Consulting Group. <https://media-publications.bcg.com/BCG-Wheres-the-Value-in-AI.pdf>

Le graphique ci-dessus représente la courbe de maturité de l'IA dans les entreprises. L'axe des abscisses est divisé en 4 tranches. La première tranche (0-25) représente les entreprises qui ne font pas ou peu de choses avec l'IA, qui ne possèdent pas les compétences pour le faire et qui par conséquent ne génèrent pas de valeur grâce à l'IA. La deuxième tranche (25-50) correspond aux entreprises qui ont développé des compétences fondamentales pour l'IA et qui ont commencé à l'expérimenter bien qu'elles aient du mal à faire croître cela et par conséquent à générer de la valeur. La troisième tranche (50-75) représente les entreprises qui ont développé une stratégie intégrant l'IA et qui ont les compétences requises pour la développer davantage. Ce sont des entreprises qui commencent à générer de la valeur grâce à l'IA. La dernière tranche (75-100) correspond aux entreprises qui sont leader en matière d'innovation et d'IA. Elles sont capables de développer des outils à la pointe de la technologie et ont les compétences requises pour générer de la valeur à partir de ceux-ci (de Bellefonds et al., 2024).

L'axe des ordonnées représente la maturité de l'entreprise en pourcentage. Nous constatons donc que lorsque les entreprises développent davantage de compétences en IA et qu'elles

commencent à générer de la valeur grâce à celle-ci, leur pourcentage de maturité augmente également (de Bellefonds et al., 2024).

Dans le cas du secteur biopharmaceutique, nous pouvons constater que le secteur se situe dans la deuxième tranche c'est-à-dire que le secteur a commencé à développer des compétences en IA mais qu'il n'est pas encore capable de générer de la valeur grâce à cela. Le secteur biopharmaceutique a environ la même maturité que le secteur de la santé, mais se situe également très proche de la moyenne, tous secteurs confondus (de Bellefonds et al., 2024).

Dans un rapport publié par Deloitte en 2025, les trois fonctions dans lesquelles l'IA est la plus avancée ont été étudiées. Il en est ressorti que, dans le secteur industriel, les fonctions liées aux opérations ont le plus grand degré d'implémentation de l'IA. Viennent ensuite les fonctions liées à l'IT et finalement les fonctions liées à la stratégie (Rowan et al., 2025).

KPMG fait le constat, dans une étude⁹ parue en 2024 que, dans l'industrie manufacturière, 23% des entreprises sont considérées comme étant débutantes en IA, 51% des entreprises l'ont implémentée et 26% des entreprises sont leader sur le plan de l'intelligence artificielle. Pour le secteur de l'énergie, des ressources naturelles et des produits chimiques, il est mentionné que 22% des entreprises sont considérées comme débutantes, 53% des entreprises l'ont implémenté et 22% sont considérées comme des leaders en IA (KPMG, 2024). Ces deux sous-secteurs faisant partie du secteur industriel, nous pouvons donc partir de l'hypothèse que la répartition globale du secteur industriel se situe dans le même ordre de grandeur que les deux secteurs mentionnés ci-dessus.

Le Digital Economy and Society Index 2022 (DESI 2022) a établi un classement du niveau d'implémentation de l'IA par secteur. Sans grand étonnement, c'est le secteur de l'information et des technologies de communications qui occupe la première place de ce classement. Le secteur manufacturier occupe la sixième place de ce classement. Malgré cela, le secteur manufacturier serait en première ligne en ce qui concerne l'adoption de nouvelles technologies (Monteiro et al., 2023).

Sur base de ces résultats, une étude¹⁰ a été menée afin de déterminer si le secteur manufacturier avait la plus grande intensité d'adoption de l'IA. Il en est ressorti que le secteur manufacturier avait effectivement un taux d'adoption de l'IA assez élevé. Ceci est confirmé par la Commission Européenne qui a mentionné que le taux d'adoption de l'IA au Portugal est remarquable (Monteiro et al., 2023).

4.4.3. Adoption de l'Intelligence Artificielle dans le contrôle interne des entreprises industrielles

Dans un rapport publié par Deloitte en 2024, nous pouvons constater que sur les 609 entreprises interrogées, tous secteurs confondus, seulement 14% d'entre elles ont tactiquement automatisé, voir hautement automatisé leurs contrôles internes. Nous pouvons donc faire l'hypothèse que

⁹ Etude réalisée auprès de 1.800 entreprises actives dans six industries, réparties dans 10 pays.

¹⁰ Etude réalisée auprès de 381 entreprises au Portugal

seule une partie de ces 14% représente l'implémentation d'intelligence artificielle car il existe d'autres moyens d'automatiser ces contrôles (Deloitte, 2024).

Dans ce même rapport, nous retrouvons une répartition du niveau de maturité digitale du contrôle interne dans les entreprises :

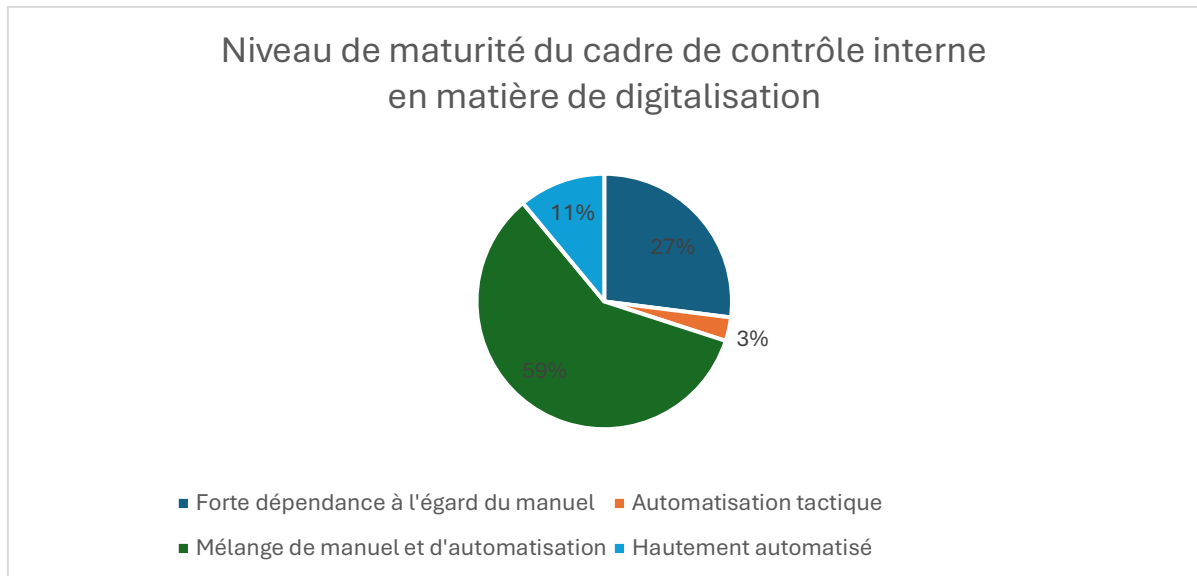


Figure 18 : Niveau de maturité du cadre de contrôle interne en matière de digitalisation (Deloitte, 2024)

Nous pouvons donc constater que près de 60% des entreprises questionnées ont actuellement une combinaison de tâches manuelles et de tâches automatisées grâce aux technologies. 27% de ces entreprises reposent quasiment uniquement sur des opérations manuelles, 3% ont mis en place une automatisation tactique et 11% ont un contrôle interne hautement automatisé. Ceci est néanmoins une représentation tous secteurs confondus et, bien que cela offre une vue d'ensemble de l'implémentation des nouvelles technologies dans le contrôle interne, nous ne pouvons pas déduire la part d'IA comprise dans ces chiffres ainsi que le secteur des entreprises répondantes (Deloitte, 2024).

D'après une étude réalisée par Supervizor¹¹ en 2024, environ 41% des entreprises utilisent ou prévoient d'utiliser de l'intelligence artificielle dans leur contrôle interne et ils prédisent que ce chiffre augmentera encore pour l'année 2025. Un autre constat qui a été fait est que les dernières versions de ChatGPT obtiennent la note de 85% lorsque nous leur faisons passer l'examen du CPA (Certified Public Accountant). Cela signifie que, techniquement, ChatGPT a obtenu ce diplôme (Supervizor, 2025).

Il n'a malheureusement pas été possible d'avoir accès à des données traitant spécifiquement du degré d'implémentation de l'IA dans le contrôle interne des entreprises industrielles. Ce degré d'implémentation spécifique au secteur industriel sera étudié plus tard dans ce travail au moyen d'une étude empirique traitant explicitement ce sujet.

¹¹ Entreprise spécialisée dans la gestion de risques financiers et la protection des entreprises face à ces risques. Elle est active en Europe et en Amérique du Nord (Supervizor, 2025).

4.4.4. Adoption de l'Intelligence Artificielle dans la gestion des risques des entreprises industrielles

Dans un rapport publié par Riskconnect¹² en 2024, nous pouvons constater que près de 90% des entreprises ont augmenté ou maintiennent leur budget pour la technologie dans la gestion des risques. Aussi, 62% des entreprises utilisent déjà de l'IA ou prévoient d'utiliser de l'intelligence artificielle dans la gestion des risques, notamment dans la prévision des risques (30%), l'évaluation des risques (29%) ainsi que dans la planification et la simulation de scénarios (27%) (Riskconnect, 2024).

De cette étude, il ressort également que la motivation principale pour l'implémentation de l'IA dans la gestion des risques est de fournir aux équipes de gestion des risques des outils technologiques leur permettant d'être plus efficaces et de se focaliser sur des missions stratégiques (Riskconnect, 2024).

Une autre étude réalisée par Riskconnect en 2024 a pour but d'évaluer les principaux cas d'utilisation de l'IA dans la gestion des risques. Le graphique ci-dessous reprend chaque cas d'utilisation et le pourcentage d'entreprises utilisant l'IA pour ces tâches.

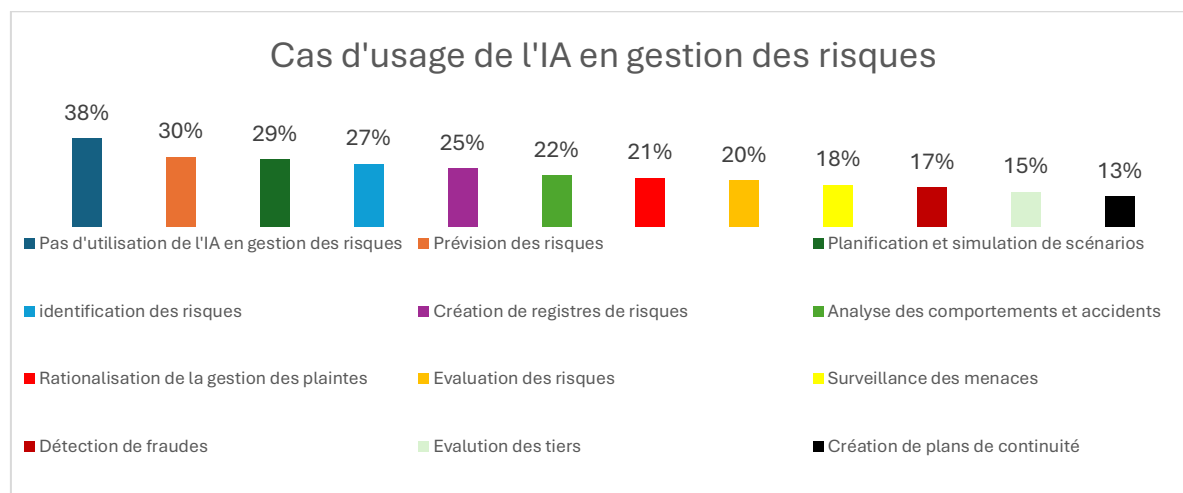


Figure 19 : Cas d'usage de l'IA en gestion des risques (Riskconnect, 2024).

Nous remarquons à l'aide de ce graphique que plus d'un tiers (38%) des entreprises n'ont pas encore utilisé d'IA dans leur gestion des risques. Nous pouvons également constater que pour 30% des entreprises, l'IA est utilisée afin de prévoir les risques auxquels elles doivent faire face. De manière générale, nous voyons que l'IA est utilisée afin d'identifier des risques ou de les répertorier et non pas d'y apporter des solutions pour les mitiger. Nous pouvons tout de même constater que 29% des entreprises utilisent l'IA afin de planifier et de simuler des scénarios ce qui peut nous laisser penser que l'IA est également implémentée dans la proposition de

¹² Fournisseur de solutions logicielles de gestion des risques active sur six continents (Riskconnect, 2025).

solutions, bien qu'elle ne serve qu'à faire des simulations sur base de ce qu'un humain a proposé comme solution (Riskconnect, 2024).

De la même manière que pour le contrôle interne, il n'a pas été possible de trouver des données spécifiques au degré d'implémentation de l'IA dans la gestion des risques. L'étude empirique développée dans la partie suivante permettra de déterminer le degré d'implémentation de l'IA dans la gestion des risques des entreprises industrielles.

4.5. Comparaison avec d'autres secteurs

Il est également intéressant de faire un parallèle entre le degré d'adoption de l'intelligence artificielle du secteur industriel et celui des autres secteurs. Ce parallèle permet de remettre en perspective l'implémentation de l'IA dans le secteur industriel et d'évaluer la performance de ce secteur en comparaison aux autres.

L'adoption de l'IA au sein des différents secteurs varie énormément. Le graphique ci-dessous permet de mieux comprendre la répartition de cette maturité de l'IA au sein de chaque secteur. Ce graphique représente la répartition des entreprises en fonction de leur maturité d'IA. Ceci sous-entend donc que les entreprises reprises pour cette étude ont toutes déjà utilisé au moins une fois de l'IA (KPMG, 2024).

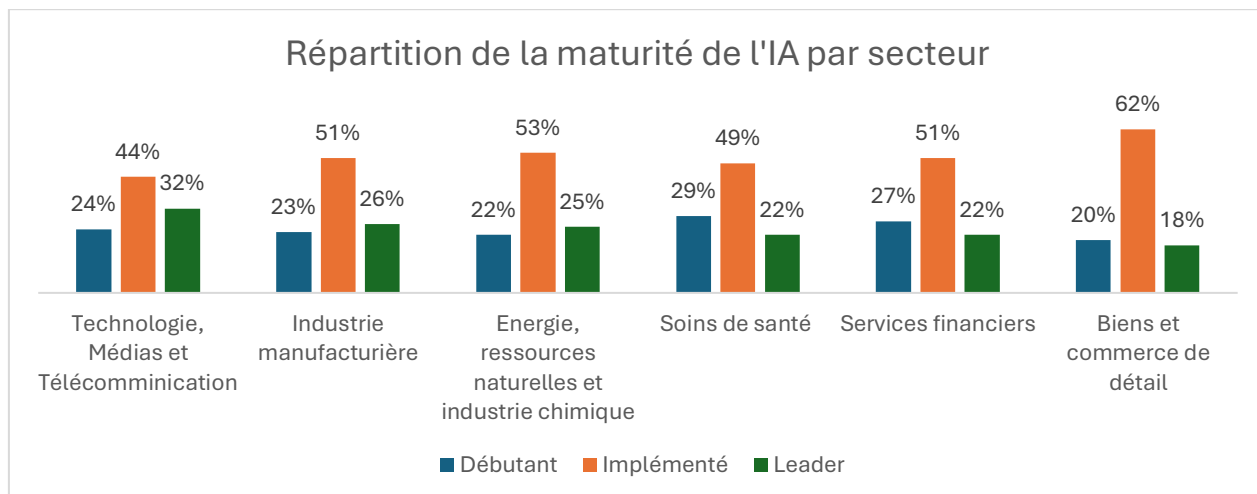


Figure 20 : Répartition de la maturité de l'IA par secteur (KPMG, 2024).

Ce graphique démontre que tous les secteurs ont une maturité plus ou moins semblable, bien que nous puissions tout de même constater que la proportion de leaders est de loin la plus importante dans le secteur de la technologie, des médias et des télécommunications avec 32% des entreprises l'ayant implémenté et générant de la valeur grâce à celle-ci. Sur ce graphique, le secteur industriel reprend l'industrie manufacturière et le secteur des énergies, des ressources naturelles et de l'industrie chimique. Cela signifie que la proportion de leaders en IA dans le secteur industriel se situe entre 25% et 26%. Le secteur ayant la moins grande proportion de leaders est le secteur de la consommation et du commerce de détail avec seulement 18%.

Néanmoins, c’est également le secteur qui a la plus grande proportion d’entreprises ayant déjà implémenté l’IA (KPMG, 2024).

Cette différence peut s’expliquer par le fait que la part du budget consacrée à l’IA est différente en fonction du secteur. Comme nous l’avons identifié ci-dessus, le secteur comptant la plus grande proportion de leaders est le secteur de la technologie, des médias et des télécommunications. C’est également le secteur qui, en moyenne investit la plus grande part de son budget dans l’IA avec 10,8% de son budget. Le secteur qui a la moins grande proportion de leaders et d’entreprises ayant implémenté l’IA est le secteur des soins de santé, et c’est également le secteur avec la plus petite part des investissements consacrés à l’IA avec seulement 9,2% (KPMG, 2024).

Le graphique ci-dessous permet d’évaluer le degré d’utilisation d’outils IA des entreprises par secteur. Il est basé sur une enquête réalisée par Vention¹³, une entreprise américaine spécialisée dans le développement d’outils numériques pour l’automatisation (Vention, 2025).

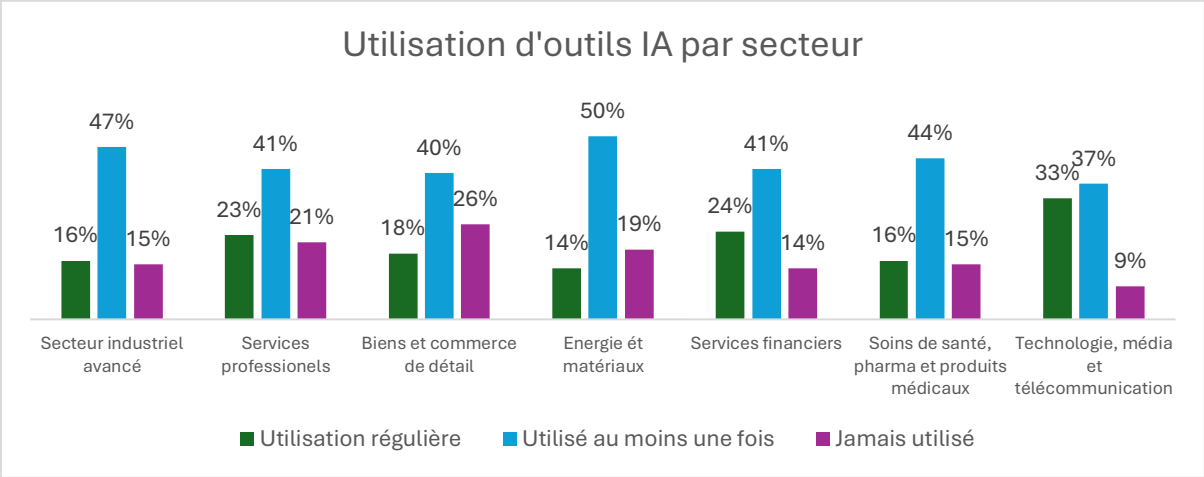


Figure 21 : Utilisation d’outils IA par secteur (Vention, 2025.).

Nous remarquons sur ce graphique que le secteur ayant implémenté l’IA à plus grande échelle est indéniablement le secteur de la technologie, des médias et des télécommunications avec 33% des entreprises de ce secteur qui utilisent l’IA de manière régulière. Le secteur industriel occupe quant à lui l’avant-dernière place avec seulement 16% des entreprises qui utilisent l’IA de manière régulière (Vention, 2025).

¹³ Entreprise américaine présente en Amérique du Nord et en Europe. Elle est experte dans les nouvelles technologies et aide ses clients à les implémenter dans leurs opérations (Vention, 2025)

5. Conclusion

L'analyse de la littérature scientifique et professionnelle nous permet de mettre en évidence plusieurs aspects de l'implémentation de l'intelligence artificielle dans la gestion des risques et du contrôle interne.

Nous avons premièrement défini le « Technology Acceptance Model », qui repose sur deux principes de base pour évaluer l'acceptation d'une nouvelle technologie d'une entreprise, à savoir l'utilité perçue et sa facilité d'utilisation. Nous avons également étudié les différents facteurs pouvant influencer l'implémentation de l'IA dans une entreprise, tels que les facteurs organisationnels et humains, les facteurs financiers, les facteurs légaux ou encore les facteurs éthiques. L'étude de ces deux points a permis de mieux comprendre les résultats obtenus dans la suite de l'étude car ils constituent une base théorique permettant d'expliquer ces résultats.

Nous avons par la suite étudié les applications de l'IA dans le contrôle interne et la gestion des risques. Cela nous a permis de comprendre que, tant dans le contrôle interne que la gestion des risques, l'IA avait de nombreuses applications dans ces domaines, notamment grâce à sa capacité d'analyse de grandes quantités d'informations, sa capacité d'identifier des modèles, mais également d'assister l'humain dans les tâches qu'il réalise. L'IA permet d'améliorer les contrôles et la gestion des risques, mais permet également de libérer du temps afin de pouvoir le consacrer à d'autres activités stratégiques.

Il est également pertinent de revenir sur les limites qui ont été identifiées pour l'implémentation de l'IA dans la gestion des risques et du contrôle interne. Ces limites sont notamment liées aux données nécessaires pour l'entraînement et l'utilisation de l'IA de manière efficace, mais également le coût initial et de fonctionnement de cette technologie. S'ajoutent à cela la nécessité d'avoir une stratégie alignée avec l'implémentation d'une IA et du personnel formé à son utilisation. Nous avons également pu relever le fait que l'IA générerait des nouveaux risques pour les entreprises tels que les « Deepfake », et une facilité croissante pour les malfaiteurs de parvenir à leurs fins.

Nous avons finalement étudié le degré d'adoption de l'IA dans le contrôle interne et la gestion des risques, ce qui nous permet de formuler une première réponse aux hypothèses formulées précédemment.

Sur base des informations récoltées, nous ne pouvons pas encore complètement confirmer la première hypothèse car nous n'avons pas pu récolter de données spécifiques à l'implémentation de l'IA dans la gestion des risques et du contrôle interne des entreprises industrielles. Néanmoins, nous pouvons estimer que ce degré d'implémentation ne sera pas très élevé. Sur base des données récoltées, nous avons pu constater que le secteur industriel n'occupait que la sixième place en termes d'implémentation de l'IA parmi l'ensemble des secteurs. De plus, l'implémentation de l'IA dans le contrôle interne et la gestion des risques n'est pas élevée non plus, bien que l'implémentation de l'IA dans la gestion des risques soit plus avancée que dans le contrôle interne. Cette réponse sera complétée dans la partie suivante grâce à une étude

empirique ciblant spécifiquement l'implémentation de l'IA dans le contrôle interne et la gestion des risques.

Concernant la deuxième hypothèse, nous pouvons, après cette étude de la littérature et des rapports, confirmer qu'il existe une relation entre la taille de l'entreprise et son degré d'implémentation de l'IA. En effet, nous avons pu constater que les grandes entreprises étaient 70% plus susceptibles d'avoir déjà implémenté l'IA que les plus petites structures.

Finalement, nous pouvons également confirmer la dernière hypothèse car en effet, nous avons pu constater que l'IA était, pour l'instant, davantage utilisée dans l'identification et la prévision des risques plutôt que dans l'élaboration de solutions. Nous avons tout de même relevé le fait que l'IA était déjà utilisée afin de faire de la planification et de la simulation, laissant sous-entendre que l'IA est tout de même utilisée dans l'élaboration de solutions, mais que ces solutions émanent d'abord des employés et qu'elles sont par la suite testées à l'aide d'une IA.

Partie V – Étude empirique

1. Objectifs

L'objectif principal de cette étude empirique est de déterminer le degré d'implémentation de l'intelligence artificielle au sein des entreprises industrielles en Belgique. L'étude empirique permettra de confronter les conclusions qui ont été faites à partir d'articles scientifiques et de rapports professionnels à des données issues du terrain. Ce parallèle permettra de confirmer les conclusions qui ont été faites lors de la revue de la littérature, ou au contraire d'y apporter des nuances. L'objectif de cette étude est également, tout comme pour la revue de la littérature, de pouvoir confirmer ou non les hypothèses qui ont été formulées.

Cette étude sera réalisée en deux parties. Nous analyserons premièrement le degré d'implémentation de l'IA dans le contrôle interne et la gestion des risques à travers une étude quantitative, permettant de mesurer directement le degré d'implémentation de l'échantillon, permettant ainsi de conclure sur l'état général de l'adoption de l'IA dans le secteur industriel belge.

Dans un second temps, nous mènerons une étude qualitative se basant sur deux interviews réalisées auprès d'experts en IA et en contrôle interne afin d'étudier leur point de vue sur la question. Cela permettra de comprendre leur ressenti, leurs attentes, mais également leurs craintes quant à l'implémentation de l'IA dans ces domaines. Cela permettra également de compléter l'étude quantitative, en apportant une explication supplémentaire quant au degré d'adoption de l'IA.

La confrontation de la revue de la littérature avec des études empiriques permettra de comprendre et d'évaluer le degré d'implémentation de l'IA dans le contrôle interne et la gestion des risques de manière générale. Ces conclusions serviront également à définir des pistes pour des recherches futures.

2. Étude quantitative

L'étude quantitative a pour objectif d'étudier le degré d'implémentation de l'intelligence artificielle dans la gestion des risques et du contrôle interne des entreprises industrielles. Comme nous avons pu le constater dans la revue de la littérature, il n'a pas été possible de récolter des données traitant précisément de l'intelligence artificielle dans le contrôle interne et la gestion des risques des entreprises industrielles. Cet outil a pour ambition de combler ce manque en étudiant de degré d'implémentation pour les industries belges.

2.1. Construction de l'outil de récolte de données

Afin de réaliser l'étude quantitative, un outil de récolte de données a été réalisé sur Microsoft Excel afin de structurer les réponses, mais également pour faciliter l'analyse des données par la suite. Cet outil est divisé en trois parties : une première partie permettant de classer les entreprises par taille, une deuxième partie permettant d'évaluer le degré d'implémentation de l'IA dans la gestion des risques et finalement une troisième partie permettant d'évaluer le degré d'implémentation de l'IA dans le contrôle interne. Cet outil préserve l'anonymat des entreprises. Par conséquent, aucune information permettant d'identifier les répondants ne sera publiée dans ce travail.

2.1.1. *Classification des entreprises par taille*

Afin de classer les entreprises en fonction de leur taille, il a été décidé d'utiliser les seuils légaux applicables en Belgique que voici (Banque Nationale de Belgique, 2025) :

Seuils pour les petites et grandes sociétés

Critère	Valeur/Nombre
Effectif de personnel, en moyenne annuelle	50 ETP (Équivalent temps plein)
Chiffre d'affaires annuel (hors tva)	11.250.000 euros
Total du bilan	6.000.000 euros

Figure 22 : Seuils pour les petites et grandes sociétés (Banque Nationale de Belgique, 2025).

- Une société est considérée comme grande si elle dépasse deux des trois critères ci-dessus.
- Une société est considérée comme petite si elle ne dépasse pas plus d'un des critères ci-dessus.

(Banque Nationale de Belgique, 2025).

Seuils pour les microsociétés

Critère	Valeur/Nombre
Effectif de personnel, en moyenne annuelle	10 ETP (Équivalent temps plein)
Chiffre d'affaires annuel (hors tva)	900.000 euros
Total du bilan	450.000 euros

Figure 23 : Seuils pour les microsociétés (Banque Nationale de Belgique 2025).

Une société est considérée comme microsociété si elle ne dépasse pas plus d'un critère ci-dessus. Une microsociété est une sous-catégorie des petites sociétés (Banque Nationale de Belgique, 2025).

2.1.2. Détermination du degré d'implémentation de l'Intelligence Artificielle

Pour déterminer le degré d'implémentation de l'IA dans les différents critères qui seront développés ci-après, il a été décidé de se baser sur le « AI assessment scale », autrement dit, échelle d'évaluation de l'IA. Cette échelle comporte 5 niveaux allant d'une utilisation nulle de l'IA à une génération complète faite par une IA. Chaque niveau est cumulatif en termes de tâches faites par l'IA. (Perkins et al., 2024).

Le tableau suivant reprend les cinq niveaux de l'échelle d'évaluation de l'IA, adaptée au contexte du contrôle interne et de la gestion des risques :

	Niveau	Description
1	Pas d'IA	Aucune intelligence artificielle n'est utilisée dans des missions de contrôle interne et de gestion des risques.
2	Assistance IA pour l'élaboration d'idées	L'IA est utilisée pour élaborer des idées de contrôle ou énoncer des potentiels risques.
3	Assistance IA pour la création	L'IA est utilisée comme assistance dans des missions de contrôle interne et de gestion des risques.
4	Tâches réalisées par l'IA et vérifiées par l'homme	L'IA effectue des contrôles internes et de la gestion des risques et l'humain vérifie les tâches réalisées par l'IA.
5	Full IA	L'IA s'occupe des contrôles internes et de la gestion des risques de manière autonome, sans intervention humaine.

Figure 24 : Échelle d'évaluation de l'IA dans le contrôle interne et la gestion des risques (Perkins et al., 2025).

2.1.3. Degré d'implémentation de l'IA dans la gestion des risques

Sur base de l'échelle présentée ci-dessus, quatre critères ont été sélectionnés afin d'évaluer le degré d'implémentation dans chacun d'entre eux. Ces critères sont basés sur le cycle de gestion des risques que nous avons développé dans la partie dédiée à la gestion des risques :

1. Identification des risques
2. Évaluation des risques
3. Contrôle (maîtrise) des risques
4. Surveillance

En se basant sur ces quatre critères, nous obtiendrons une vue d'ensemble du cycle de gestion des risques de l'entreprise, nous permettant, en plus d'évaluer le degré d'implémentation, de déterminer à quelle étape l'IA est la plus utilisée.

2.1.4. Degré d'implémentation dans le contrôle interne

Sur base de cette même échelle présentée ci-dessus, quatre critères ont été sélectionnés afin d'évaluer le degré d'implémentation de l'IA dans le contrôle interne. Ces critères sont issus du

référentiel COSO I que nous avons développé dans la partie dédiée au contrôle interne. Il a été décidé de ne pas reprendre la composante du COSO I concernant l'environnement de contrôle car ce sont davantage des caractéristiques inhérentes à l'entreprise, rendant par conséquent l'évaluation du degré d'implémentation de l'IA dans celle-ci peu pertinente. Étant donné que l'évaluation des risques était déjà reprise dans les critères pour le degré d'implémentation de l'IA dans la gestion des risques, elle a été remplacée par la détection d'anomalies.

Voici les quatre critères retenus :

1. Activités de contrôle
2. Détection d'anomalies
3. Informations et communication
4. Activités de suivi

Ces quatre critères permettront d'obtenir une vue d'ensemble du contrôle interne au sein de l'entreprise, permettant ainsi d'évaluer son degré d'implémentation en IA, mais également les tâches pour lesquelles l'IA est utilisée.

Sur base de ces huit critères, une moyenne du degré d'implémentation de l'IA en contrôle interne et gestion des risques est établie. Pour ce faire, nous avons attribué à chaque niveau de l'échelle d'évaluation de l'IA un poids :

Niveau	Poids
Pas d'IA	1
Assistance IA pour l'élaboration d'idées	2
Assistance IA pour la création	3
Tâches réalisées par l'IA et vérifiées par l'homme	5
Full IA	5

Figure 25 : Poids du niveau d'implémentation de l'IA

En calculant la moyenne des poids attribués à chacun des critères et prenant la valeur entière la plus proche, nous obtenons un nombre compris entre 1 et 5, correspondant à un niveau repris dans le tableau ci-dessus. Ceci correspond au degré d'implémentation moyen de l'IA dans le contrôle interne et la gestion des risques de l'entreprise.

2.1.5. Cible

L'étude s'est focalisée sur des entreprises industrielles belges, considérées comme des grandes entreprises au sens des seuils légaux applicables en Belgique (cf. Chapitre 2.1.1). Ces entreprises ont été sélectionnées sur base de leur taille, mais il était également important que ces entreprises soient des entreprises cotées en bourse. En effet, nous avons vu dans la partie dédiée au contrôle interne que toutes les entreprises n'avaient pas l'obligation de mettre en place un contrôle interne, même si cela est vivement conseillé. Seules les entreprises dites d'intérêt public ont cette obligation en Belgique. Il a donc semblé opportun de se focaliser sur des entreprises

cotées, afin de s'assurer qu'un contrôle interne soit en place, car dans le cas contraire, l'étude de l'entreprise n'avait que peu d'intérêt dans le cadre de ce travail.

2.2. Analyse des données

L'objectif de cette étude quantitative était d'obtenir un échantillon représentatif d'entreprises industrielles mais il n'a été possible de récolter que 7 réponses. Ce faible taux de réponses peut s'expliquer par le fait que les entreprises étaient parfois réticentes à l'idée de participer à ce genre d'enquête car elles jugeaient que les informations demandées étaient trop sensibles, malgré le fait que l'anonymat y était garanti. Ceci peut également être expliqué par le fait que le sujet de l'intelligence artificielle n'est pas un sujet maîtrisé de tous, leur empêchant ainsi de répondre de manière assurée aux questions qui leur étaient posées.

Le manque de réponses pour cette enquête quantitative restreint naturellement fortement les conclusions que nous pourrions en tirer. Néanmoins, cela fournit tout de même des données exploratoires intéressantes. Pour combler ce manque de réponses, une étude qualitative a été menée auprès de deux experts en contrôle interne et en gestion des risques. Cette étude qualitative est à retrouver dans le chapitre suivant.

Cette étude a permis de faire plusieurs constats quant à l'utilisation de l'intelligence artificielle au sein des entreprises industrielles belges.

Premièrement, nous pouvons constater que toutes les entreprises questionnées utilisent déjà de l'intelligence artificielle dans leurs activités de manière générale (Annexe 5). Néanmoins, l'utilisation de l'IA se limite aux IA génératives telles que ChatGPT ou d'autres IA similaires. Ces IA sont davantage utilisées comme moteur de recherche avancée, comme dictionnaire, ou encore comme outil de synthèse (communications personnelles, avril-mai 2025).

Nous pouvons également constater que l'ensemble des entreprises interrogées n'utilisent pas d'intelligence artificielle, tant dans la gestion des risques que du contrôle interne. Nous ne pouvons évidemment pas généraliser cela sur l'ensemble des entreprises industrielles en Belgique. Néanmoins, cette analyse se base sur les entreprises faisant, pour certaines, partie des plus importantes de Belgique en termes de chiffre d'affaires. Nous pourrions donc émettre l'hypothèse que si certaines des plus grandes entreprises industrielles de Belgique n'ont pas encore implémenté d'IA dans ces domaines, il est peu probable que des plus petites structures l'aient déjà fait. Bien entendu, cette hypothèse est à interpréter avec précaution car, comme nous l'avons déjà mentionné, l'échantillon sélectionné ne peut en aucun cas être utilisé comme échantillon représentatif (Annexe zzz).

Finalement, un autre constat qui a été marquant est que la majorité des personnes interrogées n'avaient pas de connaissance approfondie dans l'IA voire même pas de connaissances du tout. La connaissance des applications de l'IA ne dépassait que rarement la connaissance des applications de ChatGPT. Ceci démontre qu'il y a encore une énorme marge d'évolution quant à l'implémentation de l'IA dans les entreprises et plus précisément dans le contrôle interne et la

gestion des risques. Bien que, comme nous l'avons vu dans la revue de la littérature et comme nous le verrons dans l'étude qualitative, l'IA comporte des limites dans son utilisation, elle possède également énormément d'applications, permettant aux entreprises des gains de temps et donc d'argent considérables (communications personnelles, avril-mai 2025).

3. Étude qualitative

Comme mentionné dans les objectifs ci-dessus, l'étude qualitative se base sur deux interviews réalisées auprès d'experts, respectivement en intelligence artificielle dans la finance et en contrôle interne et audit interne. Ces interviews se sont avérées très intéressantes car elles permettent de comprendre de manière approfondie les raisons du degré actuel d'implémentation de l'intelligence artificielle dans le contrôle interne et la gestion des risques des entreprises industrielles belges.

3.1. Élaboration du guide d'entretien

Le guide d'entretien a été conçu dans le but d'obtenir des informations précises et fiables de l'état de l'IA dans la gestion des risques et du contrôle interne de manière générale. L'objectif était de pouvoir appuyer ou nuancer les avantages et les limites développés lors de la revue de la littérature, mais également d'avoir des avis sur l'évolution de l'IA dans les entreprises, dans l'environnement de travail et dans leurs missions.

L'objectif de ces interviews était également de pouvoir répondre aux hypothèses formulées. Par conséquent, des questions concernant l'implémentation actuelle de l'IA ont été posées, permettant de confirmer ou non la première hypothèse (cf. supra p. 39). Des questions concernant les applications actuelles les plus courantes ont également été posées, permettant de confronter la deuxième hypothèse (cf. supra p. 39). Finalement, il était intéressant d'avoir une confirmation ou non, quant à l'implication de la taille de l'entreprise dans l'implémentation de l'IA, permettant ainsi de répondre à la troisième hypothèse (cf. supra p. 39).

Pour des raisons de confidentialité, les deux personnes interviewées ont préféré rendre l'entretien anonyme, tant pour elles que pour les entreprises dans lesquelles elles travaillent. Dans ce travail nous les appellerons Expert A et Expert B.

La première interview a été réalisée avec un manager en finance (Expert A) et plus précisément en contrôle interne et en audit interne. Il est spécialisé en IA et dans le développement d'outils et de stratégies pour implémenter l'IA dans son métier de manière efficiente. Il est également la personne qui dirige entre autres l'IA dans le département et est responsable, avec d'autres, de la formation de ses collègues sur le plan de l'IA (Annexe 3).

La deuxième interview a été réalisée auprès d'un directeur en finance (Expert B) et plus particulièrement dans le département spécialisé en contrôles internes et audits internes. Son rôle est d'améliorer les contrôles internes de ses clients, mais également de les implémenter. Il est également responsable de la revue de certains contrôles internes et de missions d'assurance où il donne un avis externe sur l'environnement de contrôle de son client (Annexe 4).

Le guide d'entretien est à retrouver en Annexe 2.

3.2. Résultats de l'étude qualitative

3.2.1. *Degré d'implémentation de l'Intelligence Artificielle*

La première chose qui ressort de l'analyse qualitative est que l'intelligence artificielle a déjà un impact sur les entreprises, dans le sens où les personnes spécialisées en IA, peu importe le département, sont focalisées de façon régulière sur les manières dont l'IA peut être implémentée dans les différents services. Ces spécialistes évaluent le potentiel que l'IA peut avoir, mais également les risques que cela représente et les limites liées à cette technologie. Bien que le potentiel perçu soit important, l'implémentation actuelle de l'IA reste très limitée en Belgique (Annexe 3, Annexe 4).

Actuellement, le degré d'implémentation de l'IA dans la gestion des risques et le contrôle interne reste assez faible. Les entreprises commencent à utiliser de l'IA générative pour les assister dans la création de plans d'audit, des rapports etc. mais la maturité de ces outils est encore assez limitée au sein des entreprises. Les personnes spécialisées en IA, en contrôle interne et gestion des risques étudient de manière active les cas d'usages qui ont le plus de potentiel d'aboutir. Il a également été mentionné que l'IA permettait aujourd'hui de calculer des risques que nous n'étions pas capables de calculer auparavant. Jusqu'à présent l'IA était surtout utilisée dans la cybersécurité, la gestion des spams et du phishing, etc. (Annexe 3, Annexe 4).

Il est également ressorti des deux entretiens que la taille de l'entreprise exerçait également une influence sur le degré d'implémentation de l'IA. En effet, les plus grandes structures ont plus de moyens, tant sur le plan financier que sur le plan des ressources. L'implémentation d'un tel système est extrêmement coûteuse. De plus, il faut également des personnes spécialisées dans son implémentation et sa gestion (Annexe 3, Annexe 4).

3.2.2. *Applications de l'Intelligence Artificielle*

L'utilisation d'intelligence artificielle dans la gestion des risques et le contrôle interne offre de nombreuses applications et permettra de gagner en efficacité et en qualité. L'IA sera capable d'assister l'humain dans la réalisation de contrôles internes, mais elle permettra également de résoudre des problèmes plus complexes. Le nombre de problèmes que l'IA est capable de résoudre ne fera qu'augmenter avec le temps (Annexe 3, Annexe 4).

L'IA est capable d'analyser des quantités importantes de données en un temps restreint. Cela lui permet de générer une cartographie des risques beaucoup plus rapidement qu'auparavant. L'avantage de l'IA est que c'est une technologie qui évolue extrêmement rapidement. Les systèmes sont désormais capables de communiquer entre eux de manière plus efficace, faisant remonter les anomalies plus rapidement (Annexe 3, Annexe 4).

Il est fort probable que dans les années à venir, le système soit également capable de proposer des solutions et que l'humain n'ait plus qu'à valider la solution adéquate. Il faut tout de même mentionner le fait que, à l'heure actuelle, l'IA est davantage utilisée dans la détection d'anomalies et l'identification des risques, plutôt que dans la proposition de solutions (Annexe 3, Annexe 4).

L'IA permet également une meilleure couverture des risques et donc un meilleur contrôle, grâce à sa facilité d'utilisation et la diminution des ressources nécessaires pour mettre ces contrôles en place. L'IA permettra également de diminuer les coûts liés aux tests effectués. En effet, les tests effectués sur les contrôles sont des activités manuelles et répétitives qui prennent énormément de temps aux entreprises. L'automatisation de ces processus permettrait un gain de temps considérable, et donc une réduction des coûts. Tout ceci permet d'augmenter le degré de confiance tout en diminuant le nombre de ressources nécessaires (Annexe 3, Annexe 4)

3.2.3. Risques de l'Intelligence Artificielle

Bien entendu, l'implémentation de l'intelligence artificielle dans la gestion des risques et le contrôle interne, mais également dans les entreprises en général, entraîne des risques qu'il est important de prendre en considération.

Un premier risque est que l'IA n'est pas capable d'expliquer pourquoi elle prend une certaine décision, bien que la décision qu'elle ait prise soit la bonne. Ceci peut être problématique car cela rend la révision des décisions par un humain plus difficile. Cela peut également impliquer que l'IA se base sur des critères que l'on ne souhaite pas utiliser. Par exemple, dans le cas d'une banque qui doit accorder des prêts, une IA pourrait-être influencée dans sa décision par le genre de la personne ou encore ses origines car les données d'entraînement contenaient des biais algorithmiques. Cela sous-entend donc également un risque éthique (Annexe 4).

Un autre risque qui a été identifié est un risque lié à la formation des employés. En effet, les tâches qui sont et qui seront données à une IA sont des tâches simples et répétitives. Ce sont les tâches qui sont jusqu'à présent données à des nouveaux employés, leur permettant ainsi d'apprendre le métier et de comprendre les nuances dans chacune des tâches qu'ils font. Si l'IA se charge de ces tâches dites plus simples, cela signifie que les jeunes employés seront immédiatement confrontés à des missions plus complexes. De plus, les employés sont pour l'instant responsables de tâches plus simples et de tâches plus complexes. Si l'IA se charge des tâches plus simples, cela veut dire que les employés auront uniquement des tâches complexes à réaliser, pouvant entraîner des problèmes au sein de l'entreprise et du bien-être des employés (Annexe 4).

Il existe également des risques inhérents à l'intelligence artificielle car chaque nouvelle technologie entraîne de nouveaux risques. Un exemple concret qui a été mentionné lors de l'interview de l'Expert A était que si les entreprises utilisent de l'IA pour leur gestion des risques, cela veut dire qu'ils introduiront leurs risques dans une IA afin de trouver des solutions pour mitiger ces risques. Le risque de fuite est donc important, aggravant davantage les risques de l'entreprise, plutôt que de les mitiger. Ces risques pourraient également être réutilisés pour entraîner l'IA, ce qui pose un problème sur le plan de la confidentialité (Annexe 3).

L'IA permet également la génération de « Deepfake », c'est-à-dire des images, des vidéos ou des enregistrements vocaux fictifs. Ceux-ci peuvent être utilisés par des personnes malveillantes pour obtenir des informations confidentielles ou pour obtenir de l'argent illégalement (Annexe 3).

3.2.4. Limites de l'Intelligence Artificielle

Il existe également des limites à l'implémentation de l'IA dans la gestion des risques et du contrôle interne.

Premièrement, l'implémentation d'une IA nécessite énormément de données et ces données doivent être qualitatives. En effet, si les données sont de mauvaise qualité, les réponses que l'IA fournira seront également de mauvaise qualité. C'est ce que l'Expert A décrit comme « trash in, trash out ». L'implémentation de l'IA nécessite également des systèmes capables de réaliser tous les calculs requis. C'est pour ces raisons que son implémentation est extrêmement coûteuse (Annexe 3).

Il faudra également former les employés à son utilisation et à la compréhension du fonctionnement de cette IA. Il sera important d'avoir au sein de l'entreprise des personnes capables de comprendre le fonctionnement de l'IA et la manière dont elle est mise en place. Elles devront être en mesure de parler le même langage que les équipes informatiques, mais il sera également important de comprendre les besoins des équipes travaillant sur le terrain. De plus, il sera essentiel de garder des humains pour vérifier ce que l'IA produit comme réponses (Annexe 3, Annexe 4).

Une dernière limite qui a été identifiée est que les entreprises travaillent trop dans des « silos ». En effet, il est courant que l'équipe informatique développe ses programmes de son côté et que les équipes en finance, par exemple, doivent développer une IA de leur côté afin d'avoir un outil performant qui réponde à leurs attentes. Il sera important pour les entreprises de pouvoir sortir de ces « silos » et de communiquer avec les autres équipes pour combiner les forces. Ceci appuie encore l'importance des personnes capables de comprendre les deux langages (Annexe 3).

4. Conclusion

Les deux études empiriques qui ont été menées permettent de mettre en évidence de nombreux aspects de l'implémentation de l'intelligence artificielle dans la gestion des risques et du contrôle interne des entreprises industrielles. Elles permettent de comprendre où en sont les entreprises dans l'implémentation de l'IA de manière générale, mais également de comprendre comment l'IA est perçue par les entreprises et les spécialistes.

Nous avons pu constater au travers des différentes analyses que le degré d'implémentation de l'IA dans les entreprises est à l'heure actuelle encore assez faible. Les entreprises commencent à utiliser certains outils basés sur l'IA tels que ChatGPT ou autres applications similaires. De manière générale, la maturité des outils utilisés reste assez limitée mais les spécialistes en IA au sein des entreprises étudient de manière active les possibilités offertes.

De ces études, il est également ressorti que les applications de l'intelligence artificielle dans la gestion des risques et le contrôle interne sont nombreuses. En effet, l'IA permet d'augmenter la qualité des contrôles et de la gestion des risques tout en réduisant le temps nécessaire pour effectuer cela. L'IA permettra également de résoudre des problèmes plus complexes et de calculer des risques que nous ne pouvions pas calculer jusqu'à présent. L'IA, grâce à sa capacité d'analyser de grandes quantités de données en un temps restreint, peut avoir un impact considérable sur la manière donc les employés organiseront leur emploi du temps. Elle est capable d'effectuer des tâches simples et répétitives, qui jusqu'à présent nécessitaient un temps considérable aux employés.

Bien entendu, l'intelligence artificielle entraîne également de nouveaux risques au sein des entreprises, comme le fait qu'une IA n'est pas capable d'expliquer pourquoi elle prend une décision, rendant ainsi la révision des réponses produites difficile. Un autre risque qui a été identifié par les experts est que l'IA pourrait poser des problèmes dans la formation des nouveaux employés. En effet, si l'IA réalise les tâches simples sur lesquelles les nouveaux employés s'entraînaient initialement, comment vont-ils alors acquérir les compétences requises pour pouvoir s'occuper de tâches plus complexes ? Il se pose également la question de la charge de travail des employés car si l'IA se charge de toutes les tâches les plus simples, les employés n'auront que des tâches complexes à effectuer. Ceci pourrait avoir un impact sur le bien-être des employés au travail.

Il existe évidemment des risques inhérents à l'intelligence artificielle tels que le fait que les IA utilisent les données rentrées pour s'améliorer. Cela signifie que les risques qu'une entreprise introduit dans le système pourraient indirectement être utilisés par d'autres entreprises, voire tout simplement fuir. Ceci aggraverait les risques introduits par l'entreprise. Elle permet également de mettre au point des fraudes difficilement détectables, grâce notamment au « Deepfake ».

Cette étude a finalement permis d'identifier les limites de l'IA dans la gestion des risques et le contrôle interne. Il en est ressorti que l'IA est fortement dépendante des données utilisées pour

l'entraîner. Ces données doivent donc impérativement être qualitatives pour garantir son bon fonctionnement. C'est une des raisons pour lesquelles l'implémentation de l'IA est extrêmement coûteuse.

Une autre limite identifiée est le fait que les employés devront impérativement être formés à l'utilisation de l'IA. Il sera impératif de comprendre son fonctionnement, mais également d'avoir des personnes capables de comprendre à la fois le fonctionnement d'une IA, mais également le fonctionnement et les besoins de l'entreprise. Actuellement, les départements ne collaborent pas encore suffisamment sur le développement des IA, ce qui pourrait ralentir son déploiement.

Cette étude permet également de répondre aux différentes hypothèses qui ont été formulées précédemment.

Nous pouvons, à travers cette étude, confirmer que le degré d'adoption de l'intelligence artificielle dans le contrôle interne et dans la gestion des risques reste encore fortement limité, confirmant donc la première hypothèse (cf. supra p. 39). Néanmoins, les données récoltées ne permettent pas d'évaluer le degré exact d'adoption de l'IA dans la gestion des risques et le contrôle interne des entreprises industrielles en Belgique car nous n'avons pas pu obtenir un échantillon suffisamment important.

Cette étude nous permet de confirmer la seconde hypothèse (cf. supra p. 39) car il a été explicitement mentionné par les deux experts que la taille de l'entreprise exerçait une influence considérable sur la capacité à implémenter ce genre de technologies. Malheureusement, l'étude qualitative ne permet pas de tirer de conclusions à ce sujet.

Finalement, nous pouvons également confirmer la troisième hypothèse (cf. supra p. 39) car, à la suite des entretiens avec les experts, il en est ressorti que, à l'heure actuelle, l'IA était davantage utilisée pour l'identification et l'évaluation des risques, plutôt que dans la proposition de solutions pour mitiger ces risques. De la même manière, l'IA est davantage utilisée pour effectuer des contrôles que pour proposer des solutions en cas d'anomalies ou d'erreurs.

Partie VI – Discussion

Cette partie a pour objectif de confronter les résultats de la revue de la littérature aux résultats issus de l'étude empirique afin de déterminer dans quelles mesures les observations faites sur le terrain confirment ou nuancent les observations faites à travers la littérature. De cette manière, nous obtiendrons une vue d'ensemble objective sur le degré d'implémentation de l'intelligence artificielle dans la gestion des risques et le contrôle interne. Ces deux parties doivent être vues comme complémentaires car certaines données n'ont pas pu être trouvées sur le plan de la littérature et inversement. Cette approche croisée permet donc de combler les éventuels manquements afin d'obtenir une conclusion plus complète et précise.

Dans cette partie, nous reviendrons sur les aspects spécifiques à l'implémentation de l'intelligence artificielle dans la gestion des risques et du contrôle interne, en passant notamment en revue les applications identifiées dans chacune des études, mais également les risques et les limites liées à cela. Nous reviendrons ensuite sur les hypothèses que nous avons formulées précédemment afin de voir comment chacune de ces études contribue à la confirmation ou non de ces hypothèses.

1. Applications de l'Intelligence Artificielle

De manière générale, les applications qui ont été identifiées dans l'étude empirique sont semblables à celles identifiées dans la revue de la littérature. La capacité de l'IA à analyser des quantités de données importantes font d'elle un outil indispensable afin d'augmenter l'efficacité et la qualité des contrôles internes et de la gestion des risques.

Tant dans la revue de la littérature que dans l'étude empirique, nous avons pu identifier le fait que l'IA permettait de libérer du temps de manière considérable car elle était capable de se charger des tâches répétitives, qui nécessitaient jusqu'à présent beaucoup de temps de la part des employés.

Nous avons également pu constater le fait que l'intelligence artificielle permettait de réduire l'exposition aux risques des entreprises. Dans la revue de la littérature et les rapports publiés par des entreprises professionnelles, nous avons par exemple relevé l'assistance de l'IA dans la limitation des risques de non-conformité, mais également dans la détection d'anomalies ou de fraudes. Ceci est rendu possible grâce à la capacité de l'IA d'analyser rapidement des données.

La littérature met en avant la capacité de l'IA à prioriser certaines alertes ou risques et c'est ce que nous avons identifié dans l'étude empirique comme étant la cartographie des risques. Ceci permet à l'IA de synthétiser les risques identifiés et de les classer par ordre d'importance, mais cela permet également à l'humain d'avoir une vue d'ensemble hiérarchisée, simple à comprendre, permettant une prise de décision rapide.

2. Risques de l'Intelligence Artificielle

Ici encore, la revue de la littérature et l'étude empirique apportent des aspects complémentaires à cette analyse, mais s'accordent également sur le fait que l'implémentation de l'intelligence artificielle dans la gestion des risques et du contrôle interne engendre de nouveaux risques.

Un des risques identifiés tant par les experts lors des entretiens que dans la revue de la littérature, est celui des « Deepfake ». Les « Deepfake » sont des images, des vidéos ou encore des enregistrements vocaux réalisés à l'aide d'une IA. Ils peuvent notamment servir à des personnes malintentionnées qui se feraient passer pour une personne de confiance dans le but d'obtenir de l'argent ou encore des informations confidentielles. De manière générale, l'implémentation d'une nouvelle technologie apporte également des nouveaux risques

Lors des entretiens, d'autres risques ont également été identifiés tels que le fait qu'une intelligence artificielle ne soit pas capable d'expliquer comment elle arrive à un résultat. C'est ce que nous avons défini dans les concepts comme le phénomène de la boîte noire. Le problème avec ceci est que l'IA pourrait se baser sur des critères non-souhaités, mais cela pose également un problème pour la révision des résultats qui ont été générés par l'IA.

Ces entretiens avec des experts ont également permis de compléter les risques liés à l'implémentation de l'IA. Nous avons par exemple pu constater que la formation des employés pouvait être altérée car l'IA se chargerait des tâches simples et répétitives, or ces tâches sont nécessaires à la formation des nouvelles recrues. La réalisation des tâches les plus simples par des systèmes faisant usage de l'IA pourrait également avoir un impact sur le bien-être des employés car ceux-ci n'auront plus que des tâches lourdes à exécuter.

3. Limites de l'Intelligence Artificielle

Dans le cas des limites identifiées, tant dans la revue de la littérature que dans l'étude empirique, nous retrouvons des aspects communs mais également complémentaires.

La revue de la littérature et l'étude empirique s'alignent sur le fait que l'implémentation d'une IA dans une entreprise nécessite une quantité de données considérables et que la qualité de ces données est primordiale afin d'assurer un fonctionnement optimal du système. Les systèmes informatiques de l'entreprise doivent également être capables de supporter l'exécution des nombreux calculs et opérations. Ces deux raisons font que l'investissement initial pour implémenter une IA peut être conséquent pour une entreprise, pouvant dans certains cas constituer un frein non négligeable à son implémentation.

L'étude empirique vient compléter ces constats en ajoutant l'importance de la formation des employés à ces nouvelles technologies. Ils devront être capables de comprendre comment elles fonctionnent et comment les utiliser de manière efficace et efficiente. L'étude empirique permet également de souligner l'importance de personnes étant capables de comprendre comment gérer l'intelligence artificielle, mais également les besoins de l'entreprise afin d'adapter et d'optimiser l'IA à la société en question. Finalement, il est ressorti de l'étude empirique que les entreprises ne collaboraient pas encore assez quand il s'agit de développer des outils intégrant de l'IA car chaque département fait ses propres recherches. Il sera primordial que les départements travaillent ensemble afin de réduire les coûts et d'optimiser l'implémentation.

La revue de la littérature complète également ces limites en ajoutant le fait que l'intégration de l'IA dans une entreprises doit être en lien avec la stratégie de celle-ci. Il faut implémenter l'IA car elle apporte une plus-value à l'activité et non pas pour le simple fait de l'implémenter pour être dans l'ère du temps. La revue de la littérature a également permis de souligner le fait que l'IA manque pour l'instant encore de nuance, dans le sens où certains aspects de la gestion des risques et du contrôle interne s'appuient sur des jugements sur base de l'expérience ou du contexte, ce qu'une IA n'est pas capable de faire.

4. Hypothèses

Après avoir confronté séparément les hypothèses formulées précédemment à la revue de la littérature d'une part, et aux résultats de l'étude empirique d'autre part, il semble désormais pertinent de croiser ces deux analyses. Cette approche permet de tirer des conclusions complètes et nuancées, permettant de confirmer ou non les hypothèses avancées.

4.1. Hypothèse 1

La première hypothèse formulée met en avant que le degré d'adoption de l'intelligence artificielle dans la gestion des risques et dans le contrôle interne des entreprises industrielles est actuellement encore faible, à cause notamment du coût important de son implémentation.

Nous avons vu à travers la revue de la littérature que, de manière générale, le degré d'adoption de l'IA, tant dans le contrôle interne et la gestion des risques, que dans le secteur industriel, était encore faible et pouvait notamment s'expliquer par le coût élevé de sa mise en place. D'autres éléments tels que les facteurs organisationnels, éthiques et légaux influencent également le degré d'adoption de l'IA. La revue de la littérature n'a néanmoins pas permis d'obtenir de données spécifiques au degré d'implémentation de l'IA dans la gestion des risques et du contrôle interne des entreprises industrielles.

Les entretiens avec deux experts ont permis de confirmer le fait que ce degré d'adoption était encore faible dans les entreprises, principalement car l'investissement est conséquent et que l'entreprise doit prendre le temps de se former et de former ses employés à son utilisation. Sur base de l'étude quantitative, nous ne pouvons malheureusement pas tirer de conclusions par manque de réponses. Elle démontre tout de même que ce degré d'adoption est encore très faible dans les entreprises belges, car aucune entreprise interrogée ne l'utilise dans sa gestion des risques ou son contrôle interne.

En somme, le degré d'adoption de l'intelligence artificielle dans la gestion des risques et dans le contrôle interne des entreprises industrielles est, à l'heure actuelle, encore faible, et par manque de données, nous ne sommes pas dans la capacité d'évaluer ce degré d'adoption de manière précise.

4.2. Hypothèse 2

La deuxième hypothèse met en avant le fait que les plus grandes entreprises ont un degré d'adoption de l'intelligence artificielle plus élevé que les plus petites structures, notamment à cause de la différence de moyens financiers.

Cette hypothèse peut également être confirmée car la revue de la littérature nous a permis de constater que les entreprises de grande taille étaient 70% plus susceptibles d'avoir déjà implémenté l'IA que les plus petites entreprises.

Ceci a également été confirmé par les deux experts spécialisés en contrôle interne et en intelligence artificielle. Selon eux, cette différence est majoritairement due au fait que les plus grandes entreprises ont des moyens financiers plus importants, mais également plus d'effectifs capables de se spécialiser dans le domaine de l'IA.

L'étude quantitative ne permet malheureusement pas de faire des conclusions sur la relation entre la taille d'une entreprise et le degré d'implémentation de l'IA.

Il est également intéressant de mentionner que toute entreprise n'a pas l'obligation de mettre en place un contrôle interne. Nous avons pu constater dans la partie dédiée au contrôle interne que seules les entreprises d'intérêt public (sociétés cotées, établissements de crédit, ...) devaient mettre en place un contrôle interne, ce qui signifie donc que toute entreprise n'a pas de contrôles internes mis en place. Ceci pourrait également expliquer que les plus grandes entreprises ont un degré d'adoption plus élevé dans leur contrôle interne.

4.3. Hypothèse 3

La troisième hypothèse souligne le fait que l'IA est actuellement davantage utilisée dans l'identification et l'évaluation des risques ainsi que dans la détection d'anomalies et les activités de contrôle.

La revue de la littérature nous permet de confirmer cette hypothèse, bien que l'IA pourrait déjà être utilisée pour effectuer des simulations sur base de solutions proposées par des humains, malgré que l'IA ne soit tout de même pas capable de solutionner seule des problèmes identifiés ou encore de proposer des solutions pour mitiger les risques.

Ceci est également appuyé par les entretiens qui ont été réalisés. En effet, cette hypothèse a été confirmée explicitement par les experts, car, selon eux, l'IA est à l'heure actuelle davantage utilisée pour effectuer des contrôles.

L'étude quantitative ne permet malheureusement pas de faire des conclusions sur les tâches spécifiques du contrôle interne et de la gestion des risques dans lesquelles l'IA est implémentée.

Partie VII – Limites de l'étude

Ce mémoire comprend également certaines limites qu'il convient de souligner afin de situer la portée et la fiabilité des résultats obtenus. Ces limites sont tant liées à la méthodologie utilisée pour la réalisation de ce travail, mais également aux données utilisées et aux analyses réalisées. L'objectif de ces limites n'est pas de remettre en cause les résultats obtenus, mais bien de mettre en avant les contraintes rencontrées. Sur base de ces limites, nous développerons également des pistes de développement pour des recherches futures.

Une première limite de cette étude est la taille réduite de l'échantillon pour l'étude quantitative. En effet, il n'a été possible de récolter que 7 réponses. Comme déjà mentionné dans la partie dédiée à l'étude qualitative, ce faible taux de réponse peut s'expliquer par le fait que les entreprises étaient parfois réticentes à l'idée de transmettre des informations qu'ils jugeaient parfois sensibles, malgré la garantie de l'anonymat. Certaines entreprises n'étaient tout simplement pas dans la capacité de donner une réponse, par manque de connaissance du sujet, ou tout simplement car ils ne souhaitent pas participer à l'enquête. Ce manque de réponses a fortement limité les conclusions que nous pouvions tirer de ces données, bien que cela démontre en quelques sortes que le sujet n'est pas encore connu de tout le monde et que l'application de l'IA dans la gestion des risques et du contrôle interne n'est pas encore une pratique répandue en Belgique.

Des contraintes de temps et d'accès à certaines données ont également limité la profondeur de l'analyse de certains aspects abordés dans ce travail. Par exemple, l'analyse de la littérature n'a pas permis d'obtenir des données spécifiques au degré d'implémentation de l'IA dans le contrôle interne et la gestion des risques spécifique au secteur industriel car ces données n'existent pas ou n'ont pas fait l'objet d'une publication.

De plus, l'étude s'est focalisée sur le secteur industriel, qui est en lui-même très vaste. Il est donc fortement probable qu'il y ait des différences dans le degré d'implémentation de l'IA entre différentes activités industrielles. L'étude empirique était également focalisée sur le marché belge, limitant ainsi le nombre de données disponibles, mais également la comparaison avec d'autres pays.

Finalement, il faut souligner le fait que l'étude empirique ne s'est focalisée que sur le secteur industriel, là où la revue de la littérature a mis l'accent sur la comparaison avec d'autres secteurs. Nous n'avons pour cette partie aucune donnée empirique permettant de confirmer les conclusions faites sur base de la littérature.

Partie VIII – Pistes pour des recherches futures

Dans le but d'approfondir certains sujets abordés dans le cadre de ce travail mais également en réponse aux limites identifiées ci-dessus, cette partie a pour objectif de fournir des perspectives pour des recherches futures dans le cadre de l'implémentation de l'intelligence artificielle dans la gestion des risques et du contrôle interne des entreprises industrielles.

Il pourrait premièrement être intéressant de revoir la méthode de récolte de données dans le cadre de l'étude quantitative. Le problème rencontré dans la récolte de données est la réticence des entreprises à vouloir répondre. Nous pourrions pallier à cette réticence en changeant l'approche afin d'instaurer davantage une relation de confiance avec les entreprises. Dans le cas de ce travail, les données ont été récoltées dans la plupart du temps en face à face ou par téléphone. Afin d'instaurer une relation de confiance, nous pourrions imaginer une interview plus formelle dans laquelle nous pourrions expliquer davantage les objectifs de l'étude ainsi que les bénéfices qu'apporteraient leurs réponses à cette dernière. De cette manière, nous pourrions espérer davantage de réponses, bien que cette méthodologie nécessite considérablement plus de temps.

Il serait également intéressant d'étendre la recherche empirique à d'autres secteurs en Belgique, mais également de diviser le secteur en différentes activités. Ceci permettrait une comparaison plus complète et objective entre ceux-ci, tant dans une même industrie qu'entre différentes industries. Cette approche permettrait de remettre en perspective les différents degrés d'implémentation de l'IA en le comparant à d'autres activités ou à d'autres secteurs.

Une autre approche que nous pourrions adopter pour des futures recherches est une approche longitudinale, autrement dit, une étude permettant d'analyser le degré d'implémentation de l'IA dans le contrôle interne et la gestion des risques sur plusieurs années. Ceci permettrait d'évaluer le degré d'implémentation de l'IA sur une période plus ou moins longue, mais également de faire des prédictions sur la suite de son évolution.

Finalement, il serait intéressant d'évaluer l'évolution de la performance de la gestion des risques et du contrôle interne des entreprises ayant implémenté l'intelligence artificielle afin de voir à quel point elle permet des gains, tant sur le plan financier que sur le plan de la performance.

Partie IX – Conclusion générale

Ce travail avait pour objectif d'étudier l'impact qu'ont les nouvelles technologies sur les entreprises et plus précisément celui de l'intelligence artificielle sur le contrôle interne et la gestion des risques des entreprises industrielles.

Nous avons pu constater à travers la définition des différents concepts que le monde était en constante évolution et que les changements étaient de plus en plus rapides. Le secteur industriel lui-même a connu et connaîtra encore de nombreuses évolutions, que nous appelons révolutions industrielles. Ces révolutions font évoluer le milieu dans lequel les entreprises opèrent et métamorphosent de manière définitive la manière dont les affaires sont abordées. L'homme cherche constamment à améliorer son environnement de vie, mais également son efficacité et sa rentabilité.

L'introduction de l'intelligence artificielle ne date cependant pas d'hier. Nous entendrons parler pour la première fois des prémices de l'intelligence artificielle dans les années 1950, où Alan Turing a la volonté d'évaluer la capacité d'une machine à penser de la même manière que les humains. Depuis lors, l'intelligence artificielle a énormément évolué et c'est depuis quelques années que cette technologie s'est démocratisée et est utilisée par le grand public mais également dans les entreprises.

Il est évident que l'intelligence artificielle a un impact sur les entreprises à travers le monde et il a été intéressant de s'attarder sur l'impact de cette technologie dans une activité spécifique des entreprises à savoir la gestion des risques et le contrôle interne.

La revue de la littérature ainsi qu'une étude empirique composée d'une analyse qualitative et d'une analyse quantitative nous ont permis de répondre à la question de recherche qui avait été formulée sur base de l'étude conceptuelle, mais également de confirmer les différentes hypothèses émises.

Nous avons premièrement évalué les facteurs pouvant influencer le degré d'implémentation de l'IA dans une entreprise et en avons retenu les plus pertinents, à savoir les facteurs organisationnels et humains, les facteurs financiers, les facteurs légaux et finalement les facteurs éthiques.

La revue de la littérature couplée à l'étude empirique nous ont permis d'étudier les différentes applications qu'offrait l'intelligence artificielle dans la gestion des risques et le contrôle interne. Les éléments fondamentaux qui en sont ressortis sont le fait que la capacité de l'intelligence artificielle à analyser des quantités de données dans un temps réduit font d'elle un outil essentiel pour améliorer l'efficacité et la rentabilité des entreprises. L'IA est capable de réaliser des tâches répétitives et consommatrices de temps, libérant ainsi des employés pour des tâches à plus grande valeur ajoutée. Sa capacité d'analyse permet également aux entreprises de réduire leur exposition aux risques en améliorant les contrôles, en produisant une cartographie des risques

plus précises et de manière plus fréquente qu'avant, mais également en analysant les nouvelles réglementations auxquelles l'entreprise doit se conformer.

Bien entendu, toute nouvelle technologie engendre également des nouveaux risques et l'intelligence artificielle ne fait pas exception à la règle. Ici encore, la combinaison d'une revue approfondie de la littérature et d'une étude empirique nous ont permis d'évaluer les principaux risques liée à cette nouvelle technologie.

Il existe premièrement des risques qui sont inhérents à l'utilisation de l'intelligence artificielle dans les entreprises. Ceux-ci sont par exemple la génération de « Deepfake » ou encore une facilité accrue pour des malfaiteurs de s'introduire dans les systèmes informatiques des entreprises dans le but d'obtenir de l'argent ou des informations sensibles. Il est évident que si les entreprises sont capables d'utiliser de l'intelligence artificielle pour augmenter leurs performances, les malfaiteurs le peuvent aussi. Les entreprises doivent être préparées à cela et agir en conséquence. Il existe également un risque lié au principe de la boîte noire. En d'autres termes, une intelligence artificielle n'est pas capable d'expliquer pourquoi elle a pris une décision, même si cette décision semble être la bonne. Ceci peut poser des problèmes car ce système pourrait se baser sur des critères nous souhaités, mais cela rend la révision de la réponse par un humain bien plus difficile. Nous avons finalement relevé le fait que l'intelligence artificielle pourrait rendre la formation des nouvelles recrues plus complexes, étant donné qu'elle est capable de réaliser des tâches initialement réalisées par les nouvelles recrues dans le but d'apprendre les bases du métier.

Les limites de l'intelligence artificielle dans la gestion des risques et du contrôle interne des entreprises ne sont évidemment pas négligeables. Ce travail a permis de relever le fait que l'intelligence artificielle était fortement dépendante de la quantité de données utilisées pour l'entraîner mais également de la qualité de ces données. En plus de ces données, une IA nécessite des systèmes capables de réaliser des calculs et des opérations lourdes, mais également des employés capables de l'implémenter et de l'entretenir. Tout ceci représente un investissement considérable pour les entreprises, pouvant ainsi limiter le nombre de sociétés en mesure de l'implémenter.

Nous avons pu, à travers ce travail, remarquer que le degré d'implémentation de l'intelligence artificielle dans la gestion des risques et du contrôle interne des entreprises industrielles n'était pas encore très élevé. La plupart des entreprises industrielles ont déjà utilisé au moins une fois de l'intelligence artificielle mais dans la majeure partie des cas, cela représente l'utilisation d'intelligences artificielles génératives telles que ChatGPT ou autres IA génératives semblables. La taille de l'entreprise peut également influencer sa capacité à implémenter de l'IA dans ses systèmes. Dans les cas où l'intelligence artificielle est utilisée dans la gestion des risques et dans le contrôle interne, elle sert avant tout à identifier et évaluer les risques de l'entreprise, mais également à effectuer des contrôles.

Certaines limites doivent tout de même être soulignées dans le cadre de ce mémoire. Il est premièrement important de mentionner le fait que la taille restreinte de l'échantillon pour l'étude quantitative, résultant de la difficulté d'obtenir des réponses de la part des entreprises,

limite fortement la portée statistique de l'étude. De plus, l'étude empirique se focalise uniquement sur le secteur industriel belge, limitant ainsi la mise en perspective des résultats obtenus. Finalement, l'absence de données littéraires spécifiques à l'implémentation de l'IA dans la gestion des risques et du contrôle interne des entreprises industrielles limite également l'analyse sur ce plan-là.

Dans le prolongement de cette étude, plusieurs pistes de recherche et d'amélioration pourraient être envisagées. Premièrement, une étude qualitative menée sur un échantillon plus large permettrait de pouvoir augmenter la portée statistique de l'étude. Il pourrait également être intéressant d'élargir le spectre d'analyse et se pencher également sur d'autres secteurs afin de remettre en perspective les résultats obtenus. Il pourrait aussi être pertinent de faire cette analyse sur plusieurs années afin d'évaluer l'évolution du degré d'implémentation de l'IA dans les entreprises de différents secteurs. Finalement, il pourrait être profitable d'évaluer l'impact de l'implémentation de l'intelligence artificielle sur la performance de la gestion des risques et du contrôle interne des entreprises.

Les entreprises devront être capables d'intégrer ces innovations dans leur stratégie, mais également de prendre en compte les risques qu'elles engendrent. La maîtrise de l'intelligence artificielle constitue un levier fondamental dans la compétitivité des entreprises. La question est désormais : à quel point l'humain sera-t-il encore impliqué dans les tâches dont il est responsable ? En réalité, je pense que l'avenir ne se jouera pas entre l'humain et l'IA, mais bien dans la synergie entre les deux, permettant une gestion des risques et un contrôle interne plus rapide, plus intelligent et plus stratégique.

Bibliographie

- Agarwal, V., Gallagher, T., & Sabatini, J. (2024). *Digitizing Risk and Compliance: How AI Can Help Manage a Growing Challenge*. Harvard Business Review. <https://hbr.org/resources/pdfs/comm/pwc/DigitizingRiskAndCompliance.pdf>
- Agossah, A., Krupa, F., Perreira Da Silva, M., Deconde, G., & Le Callet, P. (2022). Déploiement de l'IA en situation de travail : une trop faible considération de l'expérience des employé-es ? *Sciences du Design*, 16(2), 68-85. Cairn.info. <https://doi.org/10.3917/sdd.016.0068>.
- Arrêté royal du 17 août 2007 relatif au contrôle interne et la gestion des risques au sein des services public. (2007, 18 octobre). *Moniteur belge*. https://www.ejustice.just.fgov.be/cgi/welcome.pl?language=fr&view_numac=AuditBoard.
- AuditBoard. (2024). *AI Adoption in the Workplace Outpaces Risk Management Strategies*. Consulté le 8 mai 2025, à l'adresse <https://auditboard.com/blog/ai-adoption-in-the-workplace-outpaces-risk-management-strategies>
- Autorité des Marchés Financiers. (2010). *Cadre de référence sur les dispositifs de gestion des risques et de contrôle interne*. <https://www.amf-france.org/fr/actualites-publications/publications/rapports-etudes-et-analyses/cadre-de-reference-sur-les-dispositifs-de-gestion-des-risques-et-de-contrôle-interne>
- Azumata. (2024). *Principaux défis et solutions pour l'industrie manufacturière en 2025*. Consulté le 14 avril 2025, à l'adresse <https://www.azumuta.com/fr/blog/top-manufacturing-industry-challenges-solutions-for-2025/>
- Baba, C., Giri, R., & Srinivasan, K. (2024). *Les pays asiatiques peuvent s'orienter vers les services pour stimuler leur croissance et leur productivité*. IMF Blog. Consulté le 14 avril 2025, à l'adresse <https://www.imf.org/fr/Blogs/Articles/2024/10/31/asias-economies-can-embrace-services-to-boost-growth-and-productivity>
- Badman, A. (2024). *Qu'est-ce que la gestion des risques liés à l'IA ?* IBM. Consulté le 13 mai 2025, à l'adresse <https://www.ibm.com/fr-fr/think/insights/ai-risk-management#:~:text=La%20gestion%20des%20risques%20par,claire%20de%20leurs%20risques%20potentiels>.
- Banque de France. (2025). *La crise de 2008*. <https://www.banque-france.fr/system/files/2025-04/Crise-2008.pdf>
- Banque Nationale de Belgique. (s.d.). *Critères de taille*. Consulté le 16 mai 2025, à l'adresse <https://www.nbb.be/fr/centrale-des-bilans/etablir-et-deposer/que-faut-il-deposer/criteres-de-taille/pour-les-societes#>
- Baudet, C., & Lebraty, J.-F. (2018). V. Fred D. Davis – L'acceptation d'un modèle par les systèmes d'information (p. 108-126). Ems; https://ezproxy.ichec.be:2394/les-grands-auteurs-en-systemes-d-information--9782376871309-page-108?site_lang=fr
- Bigham, T., Nair, S., Soral, S., Tua, A., Gallo, V., Lee, M., Mews, T., & Fouché, M. (2018). *AI and risk management*. Deloitte. <https://www.deloitte.com/global/en/Industries/financial-services/perspectives/gx-ai-and-risk-management.html>
- Boillet, J. (2018). *Why AI is both a risk and a way to manage risk*. EY. Consulté le 13 mai 2025, à l'adresse https://www.ey.com/en_it/insights/assurance/why-ai-is-both-a-risk-and-a-way-to-manage-risk
- Bokeria, G., Echter, A., & Lequai, A. (2025). *Quelles tendances pour l'Industrie en 2025 ?* Simon Kucher. Consulté le 14 avril 2025, à l'adresse <https://www.simon-kucher.com/fr/insights/industrials-sector-trends-2025>
- Bonnefous, B. (2024, novembre). Paradoxe dans l'industrie : les plans sociaux se multiplient alors que les difficultés de recrutement persistent. *Le Monde*. https://www.lemonde.fr/economie/article/2024/11/18/dans-l-industrie-les-difficultes-de-recrutement-continuent_6399581_3234.html

Bou Hamdan, R., Elias, Y., Madan, S., & Zhao, D. (2024). *How generative AI can be employed in fraud detection and prevention*. EY. <https://www.ey.com/content/dam/ey-unified-site/ey-com/en-ca/industries/financial-services/documents/ey-how-generative-ai-can-be-employed-in-fraud-detection-and-prevention.pdf>

Boubouh, I., & Ghanim, M. (2024). L'Intelligence Artificielle au Service du Contrôle Interne : Vers une Performance Organisationnelle Optimisée. *Revue Internationale des Sciences de Gestion*, 7(4), 1346-1369. <https://revue-isg.com/index.php/home/article/view/1812>

Brenet, D. (2024). *L'intelligence artificielle expliquée: Des concepts de base aux applications avancées de l'IA*. Eni.

Cabanis Dib Garrido, S., Gimonet, S., & Eudes, R. (2024). *L'intelligence artificielle, un allié du contrôle interne?* Deloitte. <https://www.deloitte.com/fr/fr/services/consulting-risk/perspectives/intelligence-artificielle-un-allie-du-contrôle-interne.html>

Capul, J.-Y., & Garnier, O. (2017). *Dico SES: L'essentiel de l'économie et des sciences sociales*. Hatier.

Climat.be. (2025). *Historique des gaz à effet de serre*. Consulté le 14 avril 2025, à l'adresse <https://climat.be/en-belgique/climat-et-emissions/emissions-des-gaz-a-effet-de-serre/historique>

Coderl, F. (2019). *Gestion des risques et contrôle interne: De la conformité à l'analyse décisionnelle*. Vuibert.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (1994). *Internal Control – Integrated Framework* Committee of Sponsoring Organizations of the Treadway Commission. Academia. https://www.academia.edu/12912529/INTERNAL_CONTROL_INTEGRATED_FRAMEWORK_Committee_of_Sponsoring_Organizations_of_the_Treadway_Commission

D-Carbonize. (2025). *Comparaison des émissions de GES par secteurs : Quels secteurs polluent le plus ?* Consulté le 14 avril 2025, à l'adresse <https://d-carbonize.eu/fr/gaz-a-effet-de-serre/comparaison-emissions-ges-secteurs/#:~:text=Le%20secteur%20industriel%20est%20responsable,grande%20quantit%C3%A9%20d'%C3%A9nergie%20fossile.>

de Bellefonds, N., Franke, M. R., Forth, P., Charanya, T., Apotheker, J., Grebe, M., Luther, A., Lukic, V., Nopp, C., de Laubier, R., Martin, M., & Sassine, J. (2024). *Where's the Value in AI?* Boston Consulting Group. <https://media-publications.bcg.com/BCG-Wheres-the-Value-in-AI.pdf>

de Soussa Cardoso, C., & Parise, F. (2023). Chapitre 3. Mettre en œuvre l'IA générative dans le contexte de l'entreprise. In *Guide de l'IA générative : Transformez votre quotidien professionnel à l'ère de ChatGPT, Bing, Bard, Bloom, Claude* (p. 71-101). De Boeck Supérieur. Cairn.info. <https://shs.cairn.info/guide-de-l-ia-generative--9782807361706-page-71?lang=fr>

Deloitte. (2024). *The Future of Controls: Becoming a Control Intelligent Organization*. <https://mkto.deloitte.com/rs/712-CNF-326/images/future-of-controls-2024.pdf?version=0>

Djossou, G. (2024). *Les industriels européens se tournent vers les Etats-Unis*. Opera Energie. Consulté le 14 avril 2025, à l'adresse <https://opera-energie.com/media/industriels-europeens-se-tournent-vers-etats-unis/>

Dugal, A., Leblanc, M., & Duprat, A. (2013). *Publication Internal Control - Integrated Framework* (2013) du COSO. <https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/cadre-de-2013-du-coso-web-v2.pdf>

Dumas, C. (s.d.). *Case study: Jérôme Kerviel and the Société Générale Scandal*. [Syllabus imprimé]. ICHEC

Edlinger, I. (2025). *Avantages et inconvénients d'un système de contrôle interne*. BOC Group. Consulté le 23 avril 2025, à l'adresse <https://www.boc-group.com/fr/blog/grc/internal-control-system-avantages-et-inconvenients/#:~:text=Inconv%C3%A9nients%20du%20syst%C3%A8me%20de%20contr%C>

3%B4le%20interne,-Voici%20les%20trois&text=perte%20de%20temps-
,La%20mise%20en%20%C5%93uvre%20d'un%20syst%C3%A8me%20de%20contr%C3%B4le
%20interne,et%20le%20maintien%20du%20syst%C3%A8me.

Ejzyn, A. (2024). *Stratégie digitale des entreprises*. [Syllabus en ligne].
<https://moodle.ichec.be/>

Floridi, L., & Cowls, J. (2019). A Unified Framework of Five Principles for AI in Society. *Harvard Data Science Review*, 1(1). <https://doi.org/10.1162/99608f92.8cd550d1>

Forum Économique Mondial. (s.d.). *Future of Jobs Report 2025 : 78 millions de nouvelles opportunités d'emploi d'ici à 2030, mais un besoin urgent d'acquisition de compétences pour préparer la main-d'œuvre*.
https://reports.weforum.org/docs/WEF_Future_of_Jobs_2025_Press_Release_FR.pdf

Fuhrer, C. (2023). Intelligence Artificielle : que dit la recherche récente? Une approche combinée bibliométrique et textuelle. *Management & Avenir*, 137(5), 89-111. Cairn.info.
<https://doi.org/10.3917/mav.137.0089>

Gaudiaut, T. (2024). *Combien pèse l'industrie dans l'économie des pays européens ?* Statista. Consulté le 14 avril 2025 à l'adresse <https://fr.statista.com/infographie/28517/part-industrie-dans-le-pib-pays-europe/>

Goetz, E. & Grandin J. (s.d.). *Lehman Brothers: La faillite du siècle*. Les Echos. Consulté le 29 mars 2025 à l'adresse https://media.lesechos.fr/infographie/lehman_brothers/

Google Deep Mind. (s.d.). *AlphaGo*. Consulté le 1 avril 2025, à l'adresse <https://deepmind.google/research/breakthroughs/alphago/>

Guigon, C. (2024). *Cartographie des risques*. Manager Go. Consulté le 19 avril 2025 à l'adresse <https://www.manager-go.com/gestion-de-projet/cartographie-des-risques.htm>

Heienickle, A. (2024). *Chronologie de ChatGPT : l'évolution des conversations basées sur l'IA*. Adogy. Consulté le 2 avril 2025, à l'adresse <https://www.adogy.com/fr/Chronologie-de-ChatGPT-L%27%C3%A9volution-des-conversations-aliment%C3%A9es-par-l%27IA/>

IBM Watson. (2021). *Global AI Adoption Index 2021*.
https://filecache.mediaroom.com/mr5mr_ibmnews/190846/IBM%27s%20Global%20AI%20Adoption%20Index%202021_Executive-Summary.pdf

IBM. (2021). *Qu'est-ce que l'IA forte?* Consulté le 10 avril 2025, à l'adresse <https://www.ibm.com/fr-fr/topics/strong-ai>

Institut National de la Statistique et des Études Économiques (INSEE). (2021). *Industrie*. Consulté le 13 avril 2025, à l'adresse <https://www.insee.fr/fr/metadonnees/definition/c1426>

Institut Supérieur de l'Environnement (ISE). (2024). *L'intelligence artificielle : une pollution cachée au cœur de l'innovation*. Consulté le 13 avril 2025, à l'adresse <https://institut-superieur-environnement.com/blog/lintelligence-artificielle-une-pollution-cachee-au-coeur-de-linnovation/>

Jha, M. (2024). *L'IA générative changera-t-elle le risque ou la réaction dans le paysage de la fraude ?* EY. Consulté le 10 mai 2025, à l'adresse https://www.ey.com/fr_ch/insights/ai/will-genai-change-risk-or-response-in-the-fraud-landscape

Jöhnk, J., Weibert, M., & Wyrski, K. (2020). Ready or Not, AI Comes - An Interview Study of Organizational AI Readiness Factors. *Bus Inf Syst Eng*, 63, 5-20. Springer Nature.
<https://doi.org/10.1007/s12599-020-00676-7>

KnowledgeLeader. (2020). *Five Components of the COSO Framework You Need to Know*. Consulté le 21 avril 2025, à l'adresse <https://info.knowledgeleader.com/bid/161685/what-are-the-five-components-of-the-coso-framework>

KPMG. (2024). *AI in financial reporting and audit: Navigating the new era*.
<https://assets.kpmg.com/content/dam/kpmgsites/xx/pdf/2024/04/ai-in-financial-reporting-and-audit-web.pdf.coredownload.inline.pdf>

La finance pour tous. (2024). *La crise des subprimes (2007-2008)*. Consulté le 29 mars 2025, à l'adresse <https://www.lafinancepourtous.com/juniors/lyceens/les-crises/la-crise-des-subprimes-2007-2008/>

Le Robert. (s.d.). Intelligence. Dans *Le Robert Dico en Ligne*. <https://dictionnaire.lerobert.com/definition/intelligence>

Loi du 7 décembre 2016 portant sur l'organisation de la profession et de la supervision publique des réviseurs d'entreprise. (2016, 13 décembre). *Moniteur belge*. https://www.ejustice.just.fgov.be/cgi/welcome.pl?language=fr&view_numac=

Mayer, H., Yee, L., Chui, M., & Roberts, R. (2025). *Superagency in the workplace: Empowering people to unlock AI's full potential*. McKinsey & Company. <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/superagency-in-the-workplace-empowering-people-to-unlock-ais-full-potential-at-work?>

Monteiro, A., Cepêda, C., Da Silva, A. C. F., & Vale, J. (2023). The Relationship between AI Adoption Intensity and Internal Control System and Accounting Information Quality. *MDPI*, 11(11). <https://doi.org/10.3390/systems11110536>

Niedercorn, F. (2019, août). 2011 Avec Watson, IBM remporte « Jeopardy ! ». *Les Echos*. <https://www.lesechos.fr/2017/08/2011-avec-watson-ibm-remporte-jeopardy-1116704>

Nuttal, K. (2025, mai). How you should calculate the ROI in AI. *The Australian*. <https://www.theaustralian.com.au/business/cfo-journal/how-you-should-calculate-the-roi-in-ai/news-story/2d2ca6bd91c442f2c7d0a12379470eef>

Odom, E. (2024). *AI Investments Climb to 10% of IT Budgets as Revenue Expectations Rise*. The National CIO Review. Consulté le 8 mai 2025, à l'adresse <https://nationalcioreview.com/articles-insights/extra-bytes/ai-investments-climb-to-10-of-it-budgets-as-revenue-expectations-rise-2/>

Paquet, G., Bawin, I., Schrooten, V., & Wattier, S. (2023-2024). *Séminaire de méthodologie et d'initiation à la démarche scientifique*. [Syllabus imprimé]. ICHEC.

Parlement européen. (2023). *Intelligence artificielle : définition et utilisation*. Consulté le 30 mars 2025, à l'adresse <https://www.europarl.europa.eu/topics/fr/article/20200827STO85804/intelligence-artificielle-definition-et-utilisation>

Perkins, M., Furze, L., Roe, J., & MacVaugh, J. (2024). The AI Assessment Scale (AIAS): A Framework For Ethical Integration Of Generative AI In Educational Assessment. *Journal of University Teaching & Learning Practice*, 21(06). <https://doi.org/10.53761/q3azde36>

Pierandrei, L. (2019). *Risk Management*. Dunod.

PlanA. (s.d.). *Que sont les critères Environnementaux, Sociaux et de Gouvernance (ESG) ?* Consulté le 14 avril 2025, à l'adresse <https://plana.earth/fr/glossaire/environnement-social-governance-esg#:~:text=ESG%20est%20l'acronyme%20de,de%20soci%C3%A9t%C3%A9%20et%20de%20gouvernance>

RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données). (2016, 4 mai). *Journal officiel de l'Union européenne*. <https://eur-lex.europa.eu/oj/direct-access.html?locale=fr>

RÈGLEMENT (UE) 2024/1689 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) no 300/2008, (UE) no 167/2013, (UE) no 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle). (2024, 17 juillet). *Journal officiel de l'Union européenne*. <https://eur-lex.europa.eu/oj/direct-access.html?locale=fr>

Riskforum.nl. (s.d.). *COSO II*. Consulté le 19 avril 2025, à l'adresse <https://riskforum.nl/encyclopedia/coso-ii/>

Riskconnect. (2024). *Eighty Percent of Organizations Don't Have a Dedicated Plan to Address Generative AI Risks, According to New Riskconnect Research*. Consulté le 13 mai 2025, à l'adresse <https://riskconnect.com/press/2024-new-generation-risk-report/>

Riskconnect. (2024). *New Survey Reveals How Organizations Are Using AI to Manage Risk*. Consulté le 13 mai 2025, à l'adresse <https://riskconnect.com/reports/using-ai-manage-risk/>

Riskconnect. (s.d.). *About Us*. Consulté le 13 mai 2025, à l'adresse <https://riskconnect.com/company/>

Rowan, J., Ammanath, B., Perricos, C., Sniderman, B., & Jarvis, D. (2025). *Now decides next: Generating a new future*. Deloitte. <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/consulting/us-state-of-gen-ai-q4.pdf>

Sengün & Partners. (2025). *Qu'est-ce qu'un crime en col blanc ?* Sengün Droit. Consulté le 19 avril 2025, à l'adresse <https://sengundroit.com/quest-ce-quun-crime-en-col-blanc/>

Shilling, C. G. (2025). *AI Implementation: Is Your Business In Compliance with Emerging Laws?* McLande Middleton. Consulté le 8 mai 2025, à l'adresse <https://www.mclane.com/insights/ai-implementation-is-your-business-in-compliance-with-emerging-laws/>

Sholtissen, B. (2024). *International Trade Finance*. [Syllabus en ligne]. ICHEC. <https://moodle.ichec.be/>

SI & Management. (s.d.). TAM, Modèle d'acceptation des technologies : difficultés et avantages perçus – F. Davis. Consulté le 6 mai 2025, à l'adresse <http://www.sietmanagement.fr/tam-modele-dacceptation-des-technologies-difficultes-percues-et-avantages-percus-f-davis/>

Société Générale. (2016). *Les 10 points clés pour comprendre l'affaire Jérôme Kerviel*. <https://www.societegenerale.com/sites/default/files/documents/proces-jk/jkerviel-10-points-fr.pdf>

Son, H. (2023). JPMorgan is developing a ChatGPT-like A.I. service that gives investment advice. CNBC. Consulté le 2 avril 2025, à l'adresse <https://www.cnbc.com/2023/05/25/jpmorgan-develops-ai-investment-advisor.htm>

Statbel. (2024). *Production industrielle*. Consulté le 14 avril 2025, à l'adresse <https://statbel.fgov.be/fr/themes/entreprises/production-industrielle#news>

Steinmetz, T. (2020). *Gestion des risques en entreprise : Le système des trois lignes de défense et ses détracteurs*. [Travail de fin d'études]. Louvain School of Management.

Stroobants, J.-P. (2025, mars). La fermeture d'Audi Brussels, symbole des difficultés de l'industrie belge. *Le Monde*. https://www.lemonde.fr/economie/article/2025/03/01/la-fermeture-d-audi-brussels-symbole-des-difficultes-de-l-industrie-belge_6571865_3234.html

Supervizor. (2025). *À propos*. Consulté le 12 mai 2025, à l'adresse <https://www.supervizor.com/fr/company/about-us>

Supervizor. (2025). *L'Intelligence artificielle en audit et contrôle interne : potentiel et limites*. Consulté le 8 mai 2025, à l'adresse <https://www.supervizor.com/fr/blog/intelligence-artificielle-audit-contrôle-interne>

Ta, P. A. (2024). *Coût de développement de l'IA : le guide ultime*. SmartDev. Consulté le 8 mai 2025, à l'adresse <https://smartdev.com/fr/ai-development-cost/>

The institute of Internal Auditors. (2024). *Le modèle des trois lignes de l'IAA : Version 2020 des Trois Lignes de Maîtrise*. <https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-french.pdf>

The Organisation for Economic Co-operation and Development (OECD). (2019). *Artificial Intelligence & responsible business conduct*. <https://mneguidelines.oecd.org/RBC-and-artificial-intelligence.pdf>

UIPath. (2025). *Robotic Process Automation (RPA)*. Consulté le 10 mai 2025, à l'adresse <https://www.uipath.com/rpa/robotic-process-automation>

University of Oxford. (2023, 5 novembre). *What is the Turing Test?* [Vidéo]. Youtube. https://www.youtube.com/watch?v=IFloRwG_d_4

Vention. (2025). *AI adoption statistics by industries and countries: 2024 snapshot*. Consulté le 13 mai 2025, à l'adresse <https://ventionteams.com/solutions/ai/adoption-statistics>

Vention. (2025). *Company*. Consulté le 13 mai 2025, à l'adresse <https://ventionteams.com/company>

Wikipédia. (2025). *Test de Turing*. Consulté le 30 mars 2025, à l'adresse https://fr.wikipedia.org/wiki/Test_de_Turing

Yol, A., (2021). *La différence entre IA, Deep Learning, Machine Learning en agriculture*. Dilepix. Consulté le 13 avril 2025, à l'adresse <https://www.dilepix.com/blog/difference-intelligence-artificielle-deep-learning-agriculture>