



OUVRAGE COLLECTIF

Management du risque et conduite du changement

Sous la direction de
Nisrine OURIACHI
Nour El Houda MOKHTARI
Majda ALAOUI

Ouvrage collectif

Management du risque et conduite du changement



Management du risque et conduite du changement



ISBN : 978-9920-213-06-6

Édition 2026



Agence Francophone

Edition et impression

Adresse électronique : francophone.agence@gmail.com

Sommaire

PREFACE.....	3
CHAPITRE 1 : <i>Les risques émergents liés à la digitalisation et leurs implications pour la fonction d’audit interne dans le secteur public</i>	6
<i>Nisrine OURIACHI ; Saadia LAARAJ</i>	
CHAPITRE 2 : <i>L’évaluation fondée sur le risque dans l’enseignement supérieur : principes, pratiques, comparaison internationale et proposition d’un modèle pour le Maroc</i>	31
<i>Abdelali Kaaouachi, Mansour Serghini,</i>	
CHAPITRE 3 : <i>Digitalisation des processus douaniers et maîtrise des risques : Enseignements pour la performance du contrôle dans le secteur public marocain</i>	51
<i>OURIACHI Nisrine ; KAMARY Nissrine</i>	
CHAPITRE 4: <i>Financial risk auditing and industrial performance: An integrative conceptual framework</i>	67
<i>Marouane EL ALITI; Omar TAOUAB</i>	
CHAPITRE 5: <i>Communication managériale et communication des risques : vers une gouvernance renouvelée à l’ère numérique</i>	82
<i>Oumayma ait moussa ; Chaymae YOUSFI</i>	
CHAPITRE 6: <i>La stratégie Leagile face aux risques logistiques : une étude empirique marocaine</i>	102
<i>Kaoutar LAMAIZI & Amina KADA</i>	
CHAPITRE 7: <i>Dispositifs de contrôle de gestion et résilience organisationnelle : quelle contribution à la maîtrise des risques dans les établissements universitaires publics ?</i>	119
<i>Loubna Fatima Zahra</i>	
CHAPITRE 8: <i>Intégration de la gestion des risques dans la planification stratégique publique au Maroc : Cadres, mécanismes et effets sur la gouvernance</i>	130
<i>BAKHTAOUI MIMOUN ; TBATIT ABDELHAMID</i>	

CHAPITRE 09: IA générative, automatisation marketing et risques numériques : une approche Design Science Research	151
Leila BAKHTI ; Ibtissam ARRASSEN ; Mohammed ERRAMDANI	
CHAPITRE 10 : Gestion du risque opérationnel lié au facteur humain dans les banques marocaines : analyse qualitative du rôle des pratiques RH	176
TAMI Amina ; SAKHRAOUI Bahija	
CHAPITRE 11 : Gestion des risques et performance des stratégies marketing omnicanales : proposition d'un modèle conceptuel dans un environnement incertain	193
AHMAME Meryem	
CHAPITRE 12 : Exploiter la transformation digitale pour rationaliser le Système de Management de la Qualité (SMQ) dans les PME : entre opportunités et risques numériques	211
Imane BOUZEGGAOUI ; Majda ALAOUI	

PREFACE

On a l'habitude de voir le risque comme une menace qu'il faut contenir, et le changement comme un mouvement qu'il faut provoquer. L'un invite à la prudence, l'autre à l'élan : les deux semblent aller en sens contraire. Or, sur le terrain, les choses sont moins tranchées. Toute transformation, qu'on la choisisse ou qu'on la subisse, crée de nouvelles zones de fragilité. Et inversement, il est rare qu'on puisse mieux gérer ses risques sans changer ses pratiques, ses réflexes, parfois même sa culture d'entreprise. Si ces deux sujets figurent dans le même ouvrage, ce n'est donc pas par simple commodité : ils renvoient à une seule et même situation, celle d'organisations qui doivent continuer à tourner tout en se transformant.

C'est cette situation qui fait objet d'exploration dans cet ouvrage collectif, « Management du risque et conduite du changement », à un moment où elle se fait particulièrement sentir. Depuis dix ans, les organisations marocaines, publiques comme privées, ont traversé des épreuves successives : crises sanitaires, drames humains, catastrophes naturelles, auxquelles se sont ajoutés l'essor rapide du numérique et l'arrivée de l'IA générative. Les équipes ont dû s'adapter vite, souvent dans l'urgence. Dans ce contexte qui ne cesse de bouger, la gestion des risques ne peut plus être laissée à quelques spécialistes : c'est l'affaire de tous. De la gouvernance aux ressources humaines, des systèmes d'information à la communication, elle repose sur une capacité essentielle, celle d'une organisation à tirer les leçons de ses propres épreuves.

Les douze chapitres de cet ouvrage abordent cette question depuis des terrains très différents, ce qui fait tout l'intérêt du volume. Le secteur public y tient une place importante, et plusieurs contributions se demandent ce que la digitalisation change concrètement pour les administrations. L'une d'elles cartographie les risques technologiques, informationnels, humains et éthiques qu'elle fait naître, et montre que l'audit interne doit élargir son champ de vision pour les prendre en compte. Une autre revient sur le cas de l'administration des douanes : la dématérialisation des procédures y a raccourci les délais et amélioré la traçabilité, mais elle n'a pas fait disparaître la sous-déclaration, ni les failles techniques. À l'échelle de l'État, un chapitre observe comment la gestion des risques a peu à peu trouvé sa place dans la planification stratégique publique : elle est bien ancrée dans le domaine budgétaire et dans la prévention des catastrophes naturelles, mais reste encore timide dans la planification sectorielle ordinaire. Enfin, deux chapitres se penchent sur l'enseignement supérieur. Le premier analyse ce que les dispositifs de contrôle de gestion apportent à la résilience des universités publiques. Le second présente l'évaluation fondée sur le risque, tire les enseignements de plusieurs expériences étrangères et propose un modèle progressif adapté au contexte marocain.

Le monde bancaire et industriel forme le second grand terrain de l'ouvrage. On y découvre comment les pratiques de gestion des ressources humaines, du recrutement à la gestion prévisionnelle des compétences, contribuent à prévenir le risque opérationnel d'origine humaine dans les banques marocaines. On y voit aussi comment la communication managériale, étudiée dans une grande banque de la place, influence la circulation de l'information sur les risques, bien au-delà des reportings officiels. Un chapitre plus théorique invite à voir l'audit des risques financiers comme une véritable capacité stratégique, qui agit sur la performance industrielle, et non comme une simple obligation de conformité. Côté industrie, une étude menée dans une

entreprise montre que la standardisation héritée du Lean et la réactivité propre à l'agilité se complètent pour affronter les aléas logistiques. Une autre contribution, consacrée aux PME, explore comment la transformation digitale peut simplifier le système de management de la qualité, sans exposer des structures aux moyens limités à des risques numériques mal maîtrisés.

Deux contributions se tournent enfin vers le marketing et les technologies émergentes. La première propose un modèle conceptuel qui relie la gestion des risques à la performance des stratégies omnicanales. La seconde, dans une démarche de design science, teste l'usage d'un modèle de langage pour transformer des représentations métier en outils numériques opérationnels. Elle rappelle qu'une telle automatisation n'a de sens que si elle s'accompagne de gouvernance, de traçabilité et d'un soutien patient auprès des équipes.

En parcourant ces contributions, on voit se dessiner plusieurs fils conducteurs qui relient les chapitres entre eux. Le premier tient à l'ambivalence du numérique : il est à la fois un levier de performance et une source de nouvelles vulnérabilités. Presque tous les auteurs le constatent, chacun depuis son terrain. Le deuxième fil concerne la place du facteur humain. Comme le formule l'un des chapitres, la résilience d'une organisation tient moins à la sophistication de ses outils qu'à la manière dont ses managers se les approprient, à la qualité de ses données et au soutien de sa gouvernance. D'autres auteurs le disent avec leurs propres mots, mais le constat est le même. Le troisième fil est sans doute le plus important : on passe d'une logique de conformité à une logique d'appropriation. Plusieurs contributions notent que les dispositifs de gestion des risques existent et sont souvent bien formalisés, mais qu'ils restent en partie à distance des décisions du quotidien. L'enjeu n'est donc plus tant de les mettre en place que de les faire vivre, et c'est précisément là que la conduite du changement retrouve toute sa place.

Cet ouvrage vise la construction patiente en rassemblant des recherches exploratoires sur des terrains marocains encore peu documentés : des entretiens en nombre limité, des cas uniques, des modèles conceptuels qui attendent d'être confrontés aux données.

Je dois dire à la fin que j'ai parcouru cette étude avec un intérêt aussi vif que soutenu, mesurant pleinement la portée et la rigueur des travaux présentés. L'ouvrage formule avec rigueur des enjeux familiers du terrain. J'ai particulièrement apprécié la centralité accordée aux exigences de fiabilité et de traçabilité des données, rappelant une réalité fondamentale : l'efficacité de la gestion repose avant tout sur la qualité de la mesure. Je souhaite que les chercheurs, les doctorants et les praticiens, auditeurs, contrôleurs, responsables qualité, cadres des administrations et des entreprises, y trouvent la même matière à réflexion, et que ce volume contribue, à sa mesure, au dialogue entre la recherche et l'action. Que les coordinateurs de l'ouvrage et l'ensemble des auteurs soient remerciés d'avoir mené ce travail à son terme et de l'offrir au débat. Mes remerciements les plus chaleureux vont tout particulièrement à Mme Nisrine Ouriachi, coordinatrice principale de ce produit, qui m'a fait le grand honneur de me confier la rédaction de cette préface.

Prof. Dr. Abdelali Kaaouachi

Directeur de l'ENCG- Oujda

Les opinions, analyses, interprétations et conclusions exprimées dans le présent ouvrage collectif n'engagent que leurs auteurs

CHAPITRE 1 : *Les risques émergents liés à la digitalisation et leurs implications pour la fonction d'audit interne dans le secteur public*

Nisrine OURIACHI Professeure chercheuse ; Saadia LAARAJ, doctorante

Entrepreneuriat, Marketing, Audit et Gouvernance -EMAG, ENCGO-UMP - Oujda

La digitalisation transforme progressivement le fonctionnement des administrations publiques en intégrant les technologies numériques dans les processus organisationnels, les modes de coordination et les dispositifs de prestation des services publics. Brennen et Kreiss (2016)¹ la définissent comme l'intégration des technologies numériques dans les pratiques sociales et organisationnelles, tandis que Mergel, et al. (2019)² montrent que, dans le secteur public, elle dépasse l'adoption d'outils techniques pour engager des ajustements organisationnels, institutionnels et managériaux.

Présentée comme un levier d'amélioration de la performance publique, la digitalisation favorise l'intégration des services, la simplification des procédures et la recomposition des relations entre l'administration et les citoyens³. Toutefois, ses effets ne sont pas automatiques, puisqu'ils dépendent des structures organisationnelles, des compétences internes et des choix de gouvernance qui accompagnent le déploiement des technologies numériques⁴. La digitalisation doit ainsi être appréhendée comme un processus socio-organisationnel complexe, porteur d'opportunités, mais aussi de risques.

Ces risques dépassent les seuls risques numériques, généralement associés aux systèmes d'information, aux données et à la cybersécurité. Ils relèvent plus largement des risques liés à la digitalisation, en intégrant des dimensions organisationnelles, humaines, sociales, éthiques et institutionnelles, telles que la résistance au changement, l'exclusion numérique ou la complexification de la responsabilité publique.

Dans ce contexte, la fonction d'audit interne se trouve directement interpellée. En tant qu'activité d'assurance et de conseil, elle contribue à l'évaluation des processus de gouvernance, de gestion des risques et de contrôle interne⁵. Or, la littérature demeure fragmentée : peu de travaux articulent simultanément les risques liés à la digitalisation dans le secteur public et leurs implications pour l'audit interne.

Cette recherche est donc orientée par la question suivante : quels sont les risques émergents liés à la digitalisation dans le secteur public et quelles implications induisent-ils pour la fonction d'audit interne ? L'article vise ainsi à identifier les principales catégories de risques liés à la

¹ Brennen et Kreiss, « Digitalization ».

² Mergel et al., « Defining Digital Transformation ».

³ Dunleavy et al., *Digital Era Governance*.

⁴ Cordella et Tempini, « E-Government and Organizational Change ».

⁵ Renard et al., *Audit interne et contrôle de gestion*.

digitalisation et à analyser les ajustements qu'elles imposent à l'audit interne, notamment en matière de cartographie des risques, de compétences numériques, de méthodes d'audit et de gouvernance numérique publique.

Revue de littérature

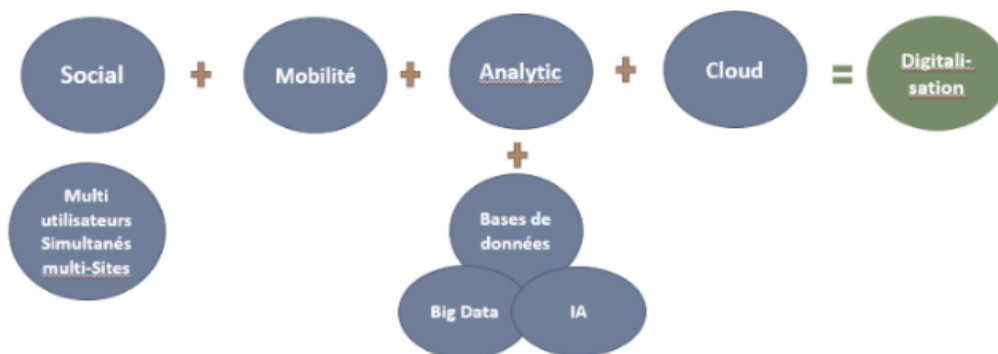
1. La digitalisation dans le secteur public

1.1. Digitalisation, numérisation et transformation digitale : clarification conceptuelle

Dans la littérature académique, la digitalisation est généralement distinguée de la numérisation et de la transformation digitale, bien que ces notions soient fréquemment utilisées de manière interchangeable dans les discours institutionnels et managériaux.

Brennen et Kreiss (2016)⁶ définissent la digitalisation comme le processus par lequel les technologies numériques sont intégrées dans les activités organisationnelles existantes, modifiant ainsi les modes de production, de coordination et de création de valeur. Elle vise à rendre les activités plus efficaces, plus agiles, plus flexibles et plus adaptées aux besoins et aux attentes des utilisateurs dans l'ère numérique⁷. Cette définition met l'accent sur l'usage organisationnel des technologies plutôt que sur leur simple dimension technique.

Figure 1 : Les outils de la digitalisation



Source : Chair, Otmane, et Samira Bounid. *Transformation digitale des systèmes de gestion comme facteur de résilience organisationnelle : Revue de littérature*.⁸

⁶ Brennen et Kreiss, « Digitalization ».

⁷ Abosson Koll et Nneme Nneme, « Comprendre la différence entre la Transformation Digitale et la Digitalisation : Revue de la littérature pour un éclairage scientifique ».

⁸ Chair et Bounid, *Transformation digitale des systèmes de gestion comme facteur de résilience organisationnelle : Revue de littérature*.

Le numérique, en revanche, se réfère aux technologies qui utilisent un codage de l'information sous forme de chiffres binaires, en opposition aux systèmes analogiques. Il inclut des dispositifs tels que les appareils photo numériques, les téléphones numériques ou tout autre équipement basé sur un traitement de données digitales⁹.

La numérisation, renvoie à une opération plus limitée, consistant en la conversion d'informations analogiques en format numérique. Elle correspond à une transformation du support de l'information, sans nécessairement impliquer une modification des processus ou des structures organisationnelles¹⁰. Autrement dit, la numérisation constitue une condition technique préalable, mais elle ne suffit pas à caractériser une dynamique organisationnelle plus large.

La digitalisation s'inscrit dans un registre différent. Elle suppose une reconfiguration des pratiques, des routines et des mécanismes de coordination autour des technologies numériques. Comme le soulignent Parviainen et al. (2012)¹¹, la digitalisation implique l'exploitation des technologies numériques afin d'améliorer les processus existants, d'accroître l'efficacité organisationnelle et de renforcer la capacité d'analyse et de pilotage. Elle introduit ainsi des changements progressifs dans les modes de fonctionnement, sans pour autant transformer nécessairement le modèle organisationnel dans son ensemble.

La transformation digitale se situe à un niveau encore plus englobant. Elle renvoie à un processus stratégique et systémique qui affecte la structure, la culture, les compétences et parfois même la finalité de l'organisation. Vial (2019)¹² la décrit comme un processus par lequel les organisations répondent aux évolutions technologiques en repensant en profondeur leurs modèles opérationnels et leur proposition de valeur. La transformation digitale dépasse l'amélioration des processus pour engager une refonte globale du modèle organisationnel Verhoef et al. (2021)¹³ afin d'y apporter de la valeur ajoutée et de sa logique de création de valeur¹⁴.

⁹ Chair et Bounid, *Transformation digitale des systèmes de gestion comme facteur de résilience organisationnelle : Revue de littérature*.

¹⁰ Tilson et al., « Research Commentary —Digital Infrastructures ».

¹¹ Parviainen et al., « Tackling the digitalization challenge ».

¹² Vial, « Understanding Digital Transformation ».

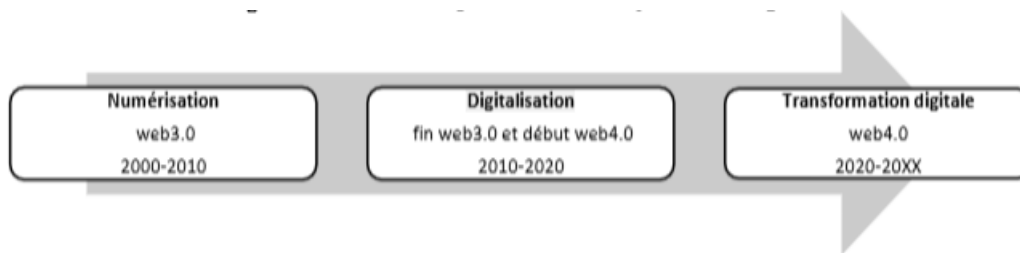
¹³ Verhoef et al., « Digital Transformation ».

¹⁴ Belhaj et al., « La transformation digitale dans les organisations publiques marocaines : Nécessité ou effet de mode ? »

Selon (Terrar, 2015) la transformation digitale peut être exprimée comme suit : « *le processus qui consiste à faire passer une organisation ayant une approche traditionnelle à de nouvelles façons de travailler et de penser en utilisant les technologies digitales, sociales, mobiles et émergentes. Elle implique un changement de leadership, une réflexion différente, la stimulation de l'innovation et de nouveaux modèles économiques, intégrant la numérisation des actifs et une utilisation accrue de la technologie pour améliorer l'expérience des employés, des clients, des fournisseurs, des partenaires et des parties prenantes de votre organisation* »¹⁵.

Ainsi, si la numérisation relève d'un changement technique, et la transformation digitale d'une mutation stratégique profonde, la digitalisation occupe une position intermédiaire : elle correspond à l'intégration progressive des technologies numériques dans les processus organisationnels existants, générant des ajustements significatifs sans impliquer nécessairement une rupture structurelle.

Figure 2 : De la numérisation à la digitalisation à la transformation digitale



Source : Fadili, Moulay Hachem, et Nawal Ilahiane. « Transition digitale ou transformation digitale : Revue de littérature pour éclairer la vision des PME et celle de leur écosystème ».¹⁶

1.2. La digitalisation dans le secteur public

Dans le secteur public, la digitalisation correspond principalement à la reconfiguration des processus administratifs à travers les technologies numériques, notamment via la dématérialisation, l'automatisation et l'interconnexion des systèmes d'information¹⁷.

Cependant, la digitalisation du secteur public ne saurait être réduite à une simple modernisation technique des procédures administratives. Elle engage également une transformation des

¹⁵ El Yaacoubi et Bennani, « Transformation digitale : quelles reconfigurations pour les métiers de la banque de détail ? »

¹⁶ Fadili et Ilahiane, « Transition digitale ou transformation digitale : Revue de littérature pour éclairer la vision des PME et celle de leur écosystème ».

¹⁷ Mergel et al., « Defining Digital Transformation ».

rapports entre l'administration, les agents publics et les usagers. À ce titre, Dunleavy et al. (2006), à travers le courant du *Digital Era Governance*¹⁸, soutiennent que l'introduction des technologies numériques dans les administrations publiques modifie les logiques de coordination, favorise l'intégration des services et redéfinit les mécanismes de responsabilité. La digitalisation devient alors un levier de recomposition institutionnelle.

Dans la même perspective, Cordella et Tempini (2015)¹⁹ soulignent que les technologies numériques ne garantissent pas automatiquement la performance. L'impact de ceux-ci est conditionné par les structures organisationnelles, les compétences internes et les décisions de gouvernance qui les accompagnent lors de leur application. En d'autres termes, la digitalisation est un processus socio-organisationnel et ne se limite pas à être un simple projet informatique.

Par conséquent, la digitalisation dans les organismes publics se présente comme une démarche hybride : elle englobe les défis techniques, organisationnels et institutionnels. C'est cette nature hybride qui explique pourquoi elle génère à la fois des opportunités d'amélioration de la performance publique et l'émergence de nouveaux risques.

2. L'audit interne à l'ère du digital

2.1 Définition de l'audit interne

La première définition de l'audit interne a été adoptée par le Conseil d'administration de l'IIA le 15 juillet 1947 et publiée dans le *Statement of Responsibilities of Internal Auditing*. Selon cette définition, l'audit interne est décrit comme « *une activité d'évaluation indépendante au sein d'une organisation, chargée d'examiner la comptabilité, la finance et les autres opérations, servant de base à des services de protection et de conseil constructif pour la direction. Il s'agit d'un type de contrôle qui fonctionne en mesurant et en évaluant l'efficacité des autres formes de contrôle. Bien qu'il soit principalement centré sur les aspects comptables et financiers, il peut également porter sur des questions opérationnelles* »²⁰.

Au fil du temps, cette conception initiale a connu d'importantes évolutions afin de s'adapter aux transformations profondes des environnements organisationnels et à l'élargissement des attentes à l'égard des fonctions de contrôle. À l'origine, l'audit interne était essentiellement orienté vers les contrôles financiers et constituait un mécanisme de vérification du respect des normes comptables et fiscales. Toutefois, sous l'effet des mutations économiques,

¹⁸ Dunleavy et al., *Digital Era Governance*.

¹⁹ Cordella et Tempini, « E-Government and Organizational Change ».

²⁰ Boudriga, *Audit interne : Organisation et Pratiques*.

technologiques et réglementaires, son champ d'intervention s'est considérablement élargi. Il intègre désormais des dimensions telles que la gestion des risques, le contrôle interne et la gouvernance.

Dans cette dynamique d'évolution, lors de la 58^e Conférence internationale en 1999, le Conseil d'administration de l'IIA a approuvé une nouvelle définition officielle de l'audit interne. Selon cette formulation actualisée, l'audit interne est : « ... *une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte des conseils pour les améliorer et contribue à la création de valeur. Il aide l'organisation à atteindre ses objectifs en évaluant, de manière systématique et méthodique, ses processus de gestion des risques, de contrôle et de gouvernance, et en formulant des recommandations destinées à renforcer leur efficacité* »²¹.

2.2. L'audit interne dans le secteur public

Dans le secteur public, l'audit interne revêt une importance particulière, car il s'inscrit dans un cadre de gouvernance élargi, où la transparence, la responsabilité et la performance sont des exigences constitutionnelles et réglementaires. Il joue le rôle de protecteur des intérêts publics en veillant à ce que les ressources soient employées efficacement, que les risques soient adéquatement identifiés et atténués, et que les procédures soient conformes aux normes éthiques et réglementaires actuelles²².

Les recherches relatives à l'audit interne dans le secteur public montrent aussi que cette fonction doit se conformer au cadre institutionnel spécifique aux administrations publiques, marqué par une diversité d'acteurs, des objectifs variés et une rigoureuse exigence de reddition des comptes. Traditionnellement, l'audit interne dans le secteur public s'est basé sur des normes et des standards internationaux valorisant l'indépendance, l'objectivité et la compétence professionnelle en tant que conditions indispensables pour fournir une assurance raisonnable contre les risques organisationnels²³. Cette reconnaissance officielle attribue à l'audit interne une place prépondérante dans le renforcement de la gouvernance publique, agissant en tant que mécanisme d'assurance et d'amélioration continue.

3. Les risques liés à la digitalisation dans le secteur public

3.1. Définitions du risque

²¹ Renard et al., *Audit interne et contrôle de gestion*.

²² Belaraj et Oukassi, « QUALITE DE L'AUDIT INTERNE AU SECTEUR PUBLIC : REVUE DE LA LITTERATURE ».

²³ Belaraj et Oukassi, « QUALITE DE L'AUDIT INTERNE AU SECTEUR PUBLIC : REVUE DE LA LITTERATURE ».

Le Petit Robert définit le risque *comme «l'éventualité d'un événement ne dépendant pas exclusivement des parties et pouvant causer la perte d'un objet ou tout autre dommage ; par extension, le risque est un événement contre la survenance duquel on s'assure »*²⁴. Nous complétons cette définition par celle du COSO-II : : « *Un risque représente la possibilité qu'un événement survienne et nuise à l'atteinte des objectifs* ». Il existe un consensus autour de la définition du risque comme « un aléa dont la survenance prive un système d'une ressource et l'empêche d'atteindre ses objectifs »²⁵.

Dans les sciences de gestion, la notion de risque est particulièrement importante dans les recherches liées à la gouvernance, au contrôle interne et à l'audit. Traditionnellement, le risque est perçu comme la possibilité qu'un événement incertain entrave l'atteinte des objectifs organisationnels. Cette définition, couramment citée dans les référentiels de gestion des risques, souligne deux aspects fondamentaux : l'incertitude et l'effet potentiel sur la performance ou la conformité.

Selon Power (2004)²⁶, les organisations modernes opèrent dans ce qu'il qualifie de « société de l'audit », où la gestion des risques s'impose comme une nécessité institutionnelle structurante. Le risque n'est plus simplement un événement aléatoire ; il se transforme en un élément de gestion formel, intégré aux dispositifs de gouvernance.

La notion de risques émergents est également introduite dans la littérature récente. Ces risques se distinguent par leur nouveauté, leur visibilité initiale limitée et leur progression rapide. Ils sont fréquemment ardues à quantifier, insuffisamment documentés et étroitement associés aux évolutions technologiques et organisationnelles. Selon Renn (2008)²⁷, les risques émergents sont souvent liés à des systèmes complexes, interconnectés et dynamiques, dans lesquels les effets domino et les dépendances mutuelles rendent les résultats ardues à prévoir. Dans un contexte de digitalisation, cette complexité est exacerbée par l'interconnexion des systèmes d'information, le flot considérable de données et l'automatisation croissante des processus décisionnels.

Par conséquent, la digitalisation ne se contente pas de produire nouveaux outils ; elle reconfigure également la nature intrinsèque du risque organisationnel. Les risques tendent à être

²⁴ BASSRIH, « Management des risques inhérents à la transformation digitale des PME ».

²⁵ Aubry et Dufour, *Risk management*.

²⁶ Power, « The Risk Management of Everything ».

²⁷ Bunting, *Global Risk Governance*, vol. 1.

de plus en plus systémiques, plus diffus et parfois moins perceptibles dans les phases préliminaires des initiatives numériques. C'est pourquoi l'analyse des risques liés à la digitalisation doit dépasser une lecture strictement technique pour intégrer également les dimensions organisationnelles, humaines, sociales, éthiques et institutionnelles.

3.2 Typologie des risques associés à la digitalisation

La digitalisation des organisations publiques entraîne une variété de risques qui dépassent le cadre strictement technologique. Les risques numériques, entendus au sens étroit, concernent principalement les systèmes d'information, la cybersécurité et les données. Toutefois, les risques liés à la digitalisation constituent une catégorie plus large, car ils englobent aussi les effets organisationnels, humains, sociaux et institutionnels produits ou accentués par l'intégration des technologies numériques dans les processus publics.

Les risques techniques et cybernétiques constituent une première catégorie. L'intégration croissante des technologies numériques transforme les structures de dépendance organisationnelle et augmente l'exposition des administrations aux vulnérabilités des systèmes d'information. Les administrations publiques deviennent ainsi plus exposées aux interruptions de service, aux pannes logicielles, aux cyberattaques ou encore aux défaillances des plateformes numériques. Ces risques peuvent compromettre la continuité du service public, la sécurité des informations et la confiance des citoyens²⁸.

Aux risques techniques s'ajoutent les risques liés aux données. L'utilisation massive des données publiques pose des problèmes de qualité, d'intégrité, de confidentialité, de traçabilité et de sécurité de l'information. Des données inexactes, incomplètes ou insuffisamment protégées peuvent nuire à la fiabilité des décisions administratives et fragiliser la légitimité de l'action publique. Janssen et van den Hoven (2015)²⁹ soulignent à cet égard l'existence d'une tension entre l'ouverture des données publiques, la transparence administrative et la protection de la vie privée. Ce paradoxe montre que la digitalisation, tout en favorisant l'accès à l'information, peut aussi générer de nouvelles vulnérabilités.

La digitalisation entraîne également des risques organisationnels. L'intégration des technologies numériques modifie les habitudes de travail, redéfinit les responsabilités et

²⁸ Bharadwaj et al., « Digital Business Strategy ».

²⁹ Janssen et Van Den Hoven, « Big and Open Linked Data (BOLD) in Government ».

transforme les circuits de décision. Selon Cordella et Tempini (2015)³⁰, les difficultés rencontrées dans les projets numériques du secteur public ne résultent pas uniquement de problèmes techniques, mais souvent d'un manque d'alignement entre les outils déployés, les structures organisationnelles existantes et les modes de gouvernance. Ce décalage peut engendrer une faible appropriation des outils, des responsabilités floues, des doublons procéduraux ou une surcharge administrative.

Les risques humains et sociaux prennent également une importance particulière. La digitalisation peut susciter des résistances lorsque les agents publics perçoivent les outils numériques comme une menace pour leurs compétences, leurs routines ou leur rôle professionnel. Elle peut aussi accentuer l'exclusion numérique de certains usagers lorsque ceux-ci ne disposent pas des équipements, des compétences ou de l'accompagnement nécessaires pour accéder aux services publics digitalisés. Ces risques montrent que la digitalisation ne concerne pas seulement les infrastructures techniques, mais aussi les capacités d'appropriation des agents et des citoyens.

Enfin, les risques éthiques et institutionnels occupent une place croissante dans les débats académiques. L'usage d'algorithmes, l'automatisation des décisions administratives et le traitement massif des données peuvent engendrer des biais, une opacité des décisions ou une difficulté d'attribution des responsabilités. Selon O'Neil (2016)³¹, les systèmes algorithmiques, lorsqu'ils sont mal conçus ou insuffisamment supervisés, peuvent produire des effets discriminatoires ou difficilement contestables par les usagers. Dans le secteur public, ces risques sont particulièrement sensibles, car l'action administrative doit respecter les principes d'égalité, de transparence, de légalité et de responsabilité.

Ces différentes catégories illustrent la nature multidimensionnelle des risques liés à la digitalisation. Ceux-ci touchent à la technologie, aux données, à l'organisation, aux comportements humains, à l'inclusion sociale, à l'éthique et à la responsabilité institutionnelle. Leur interdépendance accroît leur complexité et rend leur maîtrise plus difficile, ce qui justifie leur intégration dans les dispositifs de gouvernance, de contrôle interne et d'audit.

3.3. Spécificité des risques liés à la digitalisation dans le secteur public

³⁰ Cordella et Tempini, « E-Government and Organizational Change ».

³¹ O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*.

Dans le secteur public, les risques liés à la digitalisation présentent une spécificité particulière en raison des exigences propres à l'action administrative. Contrairement aux organisations privées, les administrations publiques doivent respecter des obligations fortes en matière de transparence, de légalité, de continuité du service public, d'égalité d'accès et de reddition des comptes. Une défaillance liée à la digitalisation ne se limite donc pas à une perte financière ou opérationnelle ; elle peut également affecter la légitimité des institutions, la protection des données personnelles, l'accessibilité des services et la confiance des citoyens.

Selon Koppell (2005), la responsabilité publique est multidimensionnelle, car elle implique à la fois la transparence, la conformité, la contrôlabilité, la réactivité et la responsabilité institutionnelle. Dans un environnement digitalisé, cette responsabilité devient plus complexe. Lorsque les décisions sont partiellement automatisées ou fondées sur des systèmes numériques interconnectés, il devient plus difficile d'identifier les responsabilités en cas d'erreur, de dysfonctionnement ou de traitement inéquitable.

Les administrations publiques se trouvent ainsi face à un paradoxe. Les technologies numériques sont mises en place pour optimiser l'efficacité, renforcer la transparence et améliorer l'accessibilité des services publics. Toutefois, lorsqu'elles sont insuffisamment maîtrisées, mal appropriées ou inégalement accessibles, elles peuvent produire des risques nouveaux, parfois peu visibles au moment de leur mise en œuvre. Cette dynamique explique pourquoi les risques liés à la digitalisation doivent être placés au cœur des débats sur la gouvernance publique, le contrôle interne et l'audit interne.

Ainsi, l'enjeu n'est pas seulement de maîtriser les risques numériques au sens technique, mais d'intégrer l'ensemble des risques liés à la digitalisation dans une approche plus globale de gouvernance. Cette perspective permet de comprendre pourquoi la fonction d'audit interne est appelée à élargir son champ d'intervention, en évaluant non seulement la sécurité des systèmes d'information, mais aussi la qualité des données, l'alignement organisationnel, l'appropriation des outils numériques, l'inclusion des usagers et la responsabilité institutionnelle.

Méthodologie de recherche

Cette recherche s'inscrit dans une démarche théorique et conceptuelle fondée sur une revue de littérature structurée. Elle repose sur une analyse organisée des contributions académiques relatives à la digitalisation du secteur public, aux risques émergents et à l'évolution de la fonction d'audit interne. Ce choix méthodologique se justifie par la nature du sujet étudié, qui

se situe à l'intersection de plusieurs champs encore partiellement fragmentés : la digitalisation des administrations publiques, la gouvernance des risques et l'audit interne.

La revue de littérature constitue une méthodologie de recherche à part entière lorsqu'elle suit une démarche explicite, rigoureuse et justifiée. Snyder (2019)³² montre qu'elle permet de synthétiser les connaissances existantes, d'identifier les zones de convergence et de tension dans un champ de recherche, ainsi que de proposer de nouvelles perspectives théoriques. Webster et Watson (2002)³³ soulignent qu'une revue de littérature ne doit pas se limiter à une description successive des travaux antérieurs, mais doit organiser les connaissances de manière conceptuelle afin de faire émerger des relations entre les notions étudiées. Tranfield, Denyer et Smart (2003)³⁴ rappellent également que les revues structurées contribuent à renforcer la transparence, la traçabilité et la robustesse des synthèses produites dans le champ du management.

Dans le cadre de cet article, la revue de littérature structurée poursuit deux finalités complémentaires. La première consiste à identifier les principales catégories de risques liés à la digitalisation dans le secteur public. La seconde vise à analyser les implications de ces risques pour la fonction d'audit interne, notamment en matière de cartographie des risques, d'évaluation des contrôles, de cybersécurité, d'adaptation des compétences, d'accompagnement du changement, d'inclusion numérique et de gouvernance publique.

La recherche documentaire a été conduite à partir de bases et sources académiques telles que Scopus, Web of Science et Google Scholar. Les mots-clés ont été mobilisés en français et en anglais afin de couvrir les principales dimensions du sujet : « digitalisation », « transformation digitale », « secteur public », « administration publique », « gouvernance numérique », « risques émergents », « risques liés à la digitalisation », « risques numériques », « cybersécurité », « audit interne », « audit public », « digital transformation », « digital risks », « internal audit » et « public sector ».

Trois critères ont été utilisés pour sélectionner les articles retenus :

- Leur pertinence en lien avec la problématique traitée ;

³² Snyder, « Literature Review as a Research Methodology ».

³³ Webster et Watson, « Analyzing the Past to Prepare for the Future ».

³⁴ Tranfield et al., « Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review ».

- Leur ancrage académique (articles scientifiques, ouvrages de référence et contributions reconnues) ;
- Leur actualité, pour intégrer les évolutions récentes en rapport avec la digitalisation.

L'analyse repose sur une lecture thématique structurée des contributions retenues. Dans un premier temps, les travaux ont été lus afin d'identifier les principales formes de risques associées à la digitalisation. Dans un deuxième temps, ces risques ont été regroupés en catégories conceptuelles : risques technologiques et cybernétiques, risques liés aux données, risques organisationnels, risques humains et sociaux, risques éthiques et institutionnels. Dans un troisième temps, ces catégories ont été mises en relation avec les missions de l'audit interne afin d'identifier les implications possibles en matière de cartographie des risques, d'évaluation des contrôles, d'adaptation des compétences, d'évolution des méthodes d'audit et d'accompagnement de la gouvernance numérique.

Cette démarche vise à proposer une synthèse structurée permettant de mieux comprendre l'évolution du rôle de l'audit interne dans un contexte de digitalisation du secteur public. Elle ne cherche pas à mesurer empiriquement l'intensité des risques étudiés, mais à construire une lecture conceptuelle cohérente des risques liés à la digitalisation et de leurs implications pour la fonction d'audit interne. Elle constitue ainsi une revue structurée à visée conceptuelle, destinée à clarifier un champ encore fragmenté et à préparer de futures recherches empiriques sur les pratiques d'audit interne face aux risques de la digitalisation.

Résultats et Discussion

4. Les risques inhérents à la digitalisation du secteur public

4.1. La résistance au changement

La résistance au changement peut représenter un obstacle majeur pour les initiatives de digitalisation des administrations publiques³⁵. La résistance à la digitalisation est donc une réaction négative résultant du traumatisme généré par la digitalisation³⁶. Elle traduit les difficultés d'adaptation des agents face aux transformations organisationnelles induites par l'introduction des outils numériques. Cette résistance peut se manifester par une inquiétude face aux nouvelles technologies, une faible appropriation des plateformes digitales, une crainte de

³⁵ BASSRIH, « Management des risques inhérents à la transformation digitale des PME ».

³⁶ Bonnet et Rappin, *Résistance et Résilience Quel couplage ?*

perte de contrôle ou encore une remise en cause de l'expertise professionnelle construite autour des pratiques traditionnelles.

Dans de nombreux contextes, les agents publics peuvent éprouver un sentiment d'inquiétude face à la digitalisation, celle-ci entraînant des perturbations des habitudes de travail et suscitant des réactions de scepticisme, voire de réticence marquée chez certains collaborateurs. Ainsi, l'organisation peut être confrontée à des attitudes défavorables lors de la mise en œuvre des outils digitaux. Cette hostilité peut se manifester sous différentes formes, allant d'un malaise discret à un refus explicite d'adopter les nouvelles technologies.³⁷ La crainte d'une perte de contrôle, d'une réduction des tâches traditionnelles ou d'une remise en cause de l'expertise professionnelle, peut conduire certains agents à limiter leur engagement dans le processus de transformation. Une telle résistance organisationnelle ralentit l'adoption des outils numériques et peut réduire significativement l'efficacité des initiatives de digitalisation dans le secteur public. Dans ces conditions, la digitalisation peut être officiellement déployée sans produire les bénéfices attendus, et engendrer des coûts ou des inefficacités plutôt qu'une véritable création de valeur.³⁸

Volodina et Grossi (2024)³⁹ soulignent que ces « peurs humaines » peuvent freiner l'évolution vers des pratiques numériques efficaces, notamment lorsque les dirigeants n'impliquent pas suffisamment les agents dans le processus de changement. La résistance au changement ne doit donc pas être comprise comme un simple comportement individuel, mais comme un risque organisationnel lié à la conduite du changement, à l'appropriation des outils et à l'alignement entre les dispositifs numériques et les pratiques réelles des agents publics.

4.2. L'exclusion numérique

L'exclusion numérique constitue une autre limite importante de la digitalisation des services publics. Elle renvoie aux difficultés rencontrées par certains usagers pour accéder aux services digitalisés, comprendre les procédures en ligne ou utiliser efficacement les outils numériques mis à leur disposition⁴⁰. Ces difficultés peuvent résulter d'un accès limité aux équipements,

³⁷ Volodina et Grossi, « Digital Transformation in Public Sector Auditing ».

³⁸ BASSRIH, « Management des risques inhérents à la transformation digitale des PME ».

³⁹ Volodina et Grossi, « Digital Transformation in Public Sector Auditing ».

⁴⁰ Djatmiko et al., « Digital Transformation and Social Inclusion in Public Services ».

d'une couverture réseau insuffisante, d'une faible maîtrise des technologies, de barrières linguistiques ou encore d'un manque d'accompagnement administratif.

Dans le secteur public, l'exclusion numérique ne constitue pas seulement un problème social. Elle devient également un risque institutionnel, car elle peut remettre en cause le principe d'égalité d'accès aux services publics. Lorsque certains citoyens ne parviennent pas à utiliser les services en ligne, la digitalisation peut produire un effet inverse à celui recherché : au lieu de rapprocher l'administration de l'utilisateur, elle peut éloigner les publics les plus vulnérables des dispositifs administratifs⁴¹.

Mesa (2023)⁴² montre que l'éducation joue un rôle important dans la capacité des citoyens à utiliser les services publics numériques et à maintenir leur confiance envers les institutions. Djatmiko, Sinaga et Pawirosumarto (2025)⁴³ soulignent également que la digitalisation peut favoriser l'inclusion sociale lorsqu'elle est accompagnée de dispositifs adaptés, mais qu'elle peut marginaliser certains publics lorsque les inégalités d'accès et de compétences ne sont pas prises en compte. L'exclusion numérique apparaît ainsi comme un risque lié à la digitalisation qui touche à la fois à l'accessibilité, à la confiance et à la légitimité de l'action publique.

4.3. La cybersécurité et la vulnérabilité des systèmes d'information

Le risque de cybersécurité constitue un facteur majeur pouvant freiner la digitalisation des organisations publiques⁴⁴. L'intégration croissante des technologies numériques accroît la dépendance des administrations publiques à leurs infrastructures digitales, à leurs plateformes de gestion, à leurs bases de données et à leurs systèmes interconnectés. Cette dépendance expose les organisations publiques à des menaces complexes, notamment les cyberattaques, les violations de données, les interruptions de service, les pannes logicielles ou les défauts de contrôle des accès⁴⁵.

Selon Volodina et Grossi (2024)⁴⁶, la digitalisation peut générer une divergence entre les aspirations technologiques et les craintes humaines, influençant la perception par les auditeurs de la mission d'audit interne. Ces risques comprennent une mauvaise intégration des procédures

⁴¹ Jacob et al., *Promesses et défis de la transformation numérique du secteur public*.

⁴² Mesa, « Digital divide, e-government and trust in public service ».

⁴³ Djatmiko et al., « Digital Transformation and Social Inclusion in Public Services ».

⁴⁴ BASSRIH, « Management des risques inhérents à la transformation digitale des PME ».

⁴⁵ Saeed et al., « Digital Transformation and Cybersecurity Challenges for Businesses Resilience ».

⁴⁶ Volodina et Grossi, « Digital Transformation in Public Sector Auditing ».

et des technologies ainsi qu'une incapacité à anticiper les risques. Dans ce contexte, l'auditeur interne dépasse désormais le simple rôle de vérificateur et agit comme un véritable acteur de création de valeur, en apportant à la direction une perspective anticipative sur les risques, notamment ceux liés à la cybersécurité.⁴⁷

Dans le secteur public, ces risques ne se limitent pas à des incidents techniques. Une attaque informatique, une indisponibilité prolongée d'un système ou une violation de données sensibles peut affecter la continuité du service public, compromettre la protection des informations personnelles et fragiliser la confiance des citoyens envers l'administration. Saeed et al. (2023)⁴⁸ montrent que la transformation numérique accroît l'exposition des organisations aux cyberattaques et aux interruptions d'activité, ce qui rend nécessaire le développement de stratégies robustes de cybersécurité.

Ces vulnérabilités peuvent également résulter d'une mauvaise intégration entre les procédures administratives et les technologies utilisées, d'un manque de coordination entre les services, d'une insuffisance des sauvegardes ou d'une faible capacité de réaction face aux incidents numériques. Dans ce contexte, la cybersécurité doit être appréhendée comme une composante des risques liés à la digitalisation, et non comme un domaine exclusivement technique relevant uniquement des spécialistes informatiques.

4.4. Les risques liés aux données

La digitalisation intensifie la production, la circulation et l'exploitation des données publiques. Ces données constituent une ressource stratégique pour améliorer la prise de décision, renforcer la traçabilité des opérations et faciliter le pilotage de l'action publique. Toutefois, leur usage massif soulève plusieurs risques liés à la qualité, à l'intégrité, à la confidentialité, à la sécurité et à la traçabilité de l'information.

Une donnée inexacte, incomplète, obsolète ou insuffisamment protégée peut fragiliser la fiabilité des décisions administratives. De même, une circulation mal contrôlée des données peut exposer l'administration à des risques juridiques, éthiques et réputationnels. Janssen et van den Hoven (2015)⁴⁹ montrent que l'ouverture et l'interconnexion des données publiques créent

⁴⁷ Ouhoud et El Ouafa, « Le rôle transformationnel de l'intelligence artificielle dans l'audit interne à l'ère du digital ».

⁴⁸ Saeed et al., « Digital Transformation and Cybersecurity Challenges for Businesses Resilience ».

⁴⁹ Janssen et Van Den Hoven, « Big and Open Linked Data (BOLD) in Government ».

une tension entre transparence administrative, efficacité de l'action publique et protection de la vie privée.

Dans ce sens, les risques liés aux données doivent être considérés comme une catégorie spécifique des risques liés à la digitalisation. Ils ne relèvent pas uniquement de la sécurité informatique ; ils concernent également la gouvernance de l'information, la responsabilité des acteurs, la qualité des traitements et la conformité aux principes de protection des données personnelles.

4.5. Les risques éthiques et institutionnels

La digitalisation du secteur public soulève enfin des risques éthiques et institutionnels. L'usage d'algorithmes, l'automatisation partielle de certaines décisions administratives et le recours croissant aux systèmes numériques peuvent produire des effets d'opacité, de biais ou de discrimination lorsqu'ils sont insuffisamment contrôlés. O'Neil (2016)⁵⁰ montre que les systèmes algorithmiques peuvent générer des conséquences discriminatoires ou difficilement contestables lorsqu'ils reposent sur des modèles opaques ou mal supervisés.

Dans le secteur public, ces risques sont particulièrement sensibles, car les décisions administratives doivent respecter les principes de légalité, d'égalité, de transparence et de responsabilité. Lorsqu'une décision dépend d'un système automatisé, d'une base de données ou d'un traitement algorithmique, il peut devenir plus difficile d'identifier clairement les responsabilités en cas d'erreur ou de traitement inéquitable. Koppell (2005)⁵¹ rappelle que la responsabilité publique est multidimensionnelle, puisqu'elle implique à la fois la transparence, la conformité, la contrôlabilité, la réactivité et la responsabilité institutionnelle.

Ces risques éthiques et institutionnels montrent que la digitalisation ne transforme pas seulement les outils de gestion publique ; elle modifie également les conditions de légitimité, de contrôle et de reddition des comptes. Leur prise en compte devient donc indispensable dans toute réflexion sur la gouvernance publique digitalisée.

5. Les implications de la digitalisation pour la fonction d'audit interne dans le secteur public

5. 1. L'audit interne et la maîtrise du risque de résistance au changement

⁵⁰ O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*.

⁵¹ Koppell, « Pathologies of Accountability ».

La digitalisation des organisations publiques constitue un processus socio-organisationnel qui perturbe les routines professionnelles, redéfinit les responsabilités et modifie les équilibres institutionnels. Les travaux sur le changement organisationnel montrent que les échecs des projets de transformation ne sont pas uniquement imputables aux défaillances technologiques ; ils peuvent également résulter de résistances internes, de défauts d'appropriation et d'insuffisances dans la conduite du changement⁵². Dans le secteur public, ces résistances peuvent être accentuées par la rigidité des procédures, la pluralité des acteurs et les exigences de conformité qui encadrent l'action administrative.

L'introduction de dispositifs numériques tend ainsi à produire des tensions liées à la redéfinition des rôles, à la perte perçue d'expertise ou à l'incertitude sur les compétences futures⁵³. Volodina et Grossi (2025)⁵⁴ montrent que la digitalisation dans l'audit public suscite à la fois des attentes d'amélioration et des craintes humaines liées à l'adaptation des pratiques professionnelles.

Dans ce contexte, l'audit interne peut contribuer à la maîtrise du risque de résistance au changement. Il peut évaluer la maturité organisationnelle, la cohérence des dispositifs de formation, le niveau d'implication des agents, l'adéquation des outils numériques aux besoins opérationnels et l'adaptation des contrôles internes aux nouvelles pratiques digitales. L'audit interne ne se limite donc pas à une vérification ex post ; il peut également apprécier la capacité de l'organisation à intégrer les outils numériques dans ses processus, à accompagner les agents et à réduire les blocages susceptibles de freiner la digitalisation.

5.2. L'audit interne et l'exclusion numérique

L'essor de la digitalisation des services publics peut accentuer les disparités d'accès aux dispositifs administratifs, notamment lorsque les compétences, les équipements ou les moyens numériques des usagers demeurent inégaux. L'exclusion numérique constitue alors un risque lié à la digitalisation, car elle peut éloigner certains citoyens des services publics au lieu de faciliter leur accès. Elle peut résulter d'un accès limité aux équipements, d'une couverture réseau insuffisante, d'une faible maîtrise des technologies, de barrières linguistiques ou encore d'un manque d'accompagnement administratif.

Dans le secteur public, l'exclusion numérique ne constitue pas seulement un enjeu social. Elle devient également un risque institutionnel, organisationnel et réputationnel, dans la mesure où

⁵² Kotter, *Leading change*; Armenakis et Bedeian, « Organizational Change ».

⁵³ Wirtz et al., « E-Participation ».

⁵⁴ Volodina et Grossi, « Digital Transformation in Public Sector Auditing ».

elle peut remettre en cause le principe d'égalité d'accès aux services publics, affaiblir la confiance des citoyens et générer des réclamations. Mesa (2023)⁵⁵ montre que l'éducation joue un rôle important dans la capacité des citoyens à utiliser les services publics numériques et à maintenir leur confiance envers les institutions. Djatmiko, Sinaga et Pawirosumarto (2025)⁵⁶ soulignent également que la digitalisation peut favoriser l'inclusion sociale lorsqu'elle s'accompagne de dispositifs adaptés, mais qu'elle peut marginaliser certains publics lorsque les inégalités d'accès et de compétences ne sont pas prises en compte.

L'audit interne est donc appelé à intégrer l'exclusion numérique dans son champ d'évaluation. Il peut examiner l'accessibilité des services numériques, l'existence de canaux alternatifs pour les usagers vulnérables, la disponibilité de dispositifs d'assistance, la simplicité des procédures en ligne et la cohérence des stratégies d'inclusion digitale.

5.3. L'audit interne et les risques liés à la sécurité des systèmes d'information

La digitalisation accroît la dépendance des administrations publiques aux systèmes d'information interconnectés, aux plateformes numériques et aux bases de données. Cette interdépendance génère des vulnérabilités systémiques, notamment en matière de cyberattaques, d'interruptions de service, de compromission des données et de défaillance des dispositifs de contrôle des accès. Saeed et al. (2023)⁵⁷ montrent que la transformation numérique expose les organisations à des risques accrus de cyberattaques, de violations de données et d'interruptions d'activité.

Dans le secteur public, ces risques prennent une importance particulière, car la sécurité des systèmes d'information conditionne la continuité du service public, la protection des données sensibles et la confiance des citoyens.

L'audit interne est donc appelé à évaluer la robustesse des dispositifs de sécurité des systèmes d'information, l'efficacité des procédures de prévention, la gestion des droits d'accès, les mécanismes de sauvegarde, les plans de continuité d'activité et la capacité de réaction face aux incidents numériques. Steinbart et al. (2018)⁵⁸ montrent que la qualité de la relation entre l'audit interne et la fonction de sécurité de l'information peut améliorer les résultats en matière de

⁵⁵ Mesa, « Digital divide, e-government and trust in public service ».

⁵⁶ Djatmiko et al., « Digital Transformation and Social Inclusion in Public Services ».

⁵⁷ Saeed et al., « Digital Transformation and Cybersecurity Challenges for Businesses Resilience ».

⁵⁸ Steinbart et al., « The Influence of a Good Relationship between the Internal Audit and Information Security Functions on Information Security Outcomes ».

sécurité organisationnelle. Ainsi, l'audit interne ne doit pas considérer la cybersécurité comme un domaine exclusivement technique ; il doit l'intégrer dans une approche globale de gouvernance, de contrôle interne et de gestion des risques liés à la digitalisation.

5.4. L'audit interne et la gouvernance des données

La digitalisation du secteur public intensifie la production, la circulation et l'exploitation des données administratives. Ces données deviennent une ressource stratégique pour améliorer la prise de décision, assurer la traçabilité des opérations et renforcer la qualité des services publics. Toutefois, elles génèrent également des risques liés à leur qualité, leur intégrité, leur confidentialité, leur traçabilité et leur protection.

Janssen et van den Hoven (2015)⁵⁹ soulignent que l'ouverture et l'interconnexion des données publiques créent une tension entre transparence administrative, efficacité publique et protection de la vie privée. Une donnée inexacte, incomplète ou insuffisamment protégée peut fragiliser la fiabilité des décisions administratives et nuire à la légitimité de l'action publique.

Dans ce contexte, l'audit interne peut jouer un rôle important dans l'évaluation de la gouvernance des données. Il peut examiner les règles de collecte, de traitement, de stockage, de partage et de protection des données. Il peut également apprécier la traçabilité des traitements, la qualité de l'information utilisée dans les processus décisionnels et la conformité des pratiques aux exigences de confidentialité et de responsabilité publique.

5.5. L'audit interne face aux risques éthiques et institutionnels

La digitalisation soulève également des risques éthiques et institutionnels, notamment lorsque les décisions administratives reposent sur des systèmes automatisés, des traitements algorithmiques ou des bases de données interconnectées. Ces dispositifs peuvent produire des effets d'opacité, de biais ou de discrimination lorsqu'ils ne sont pas suffisamment contrôlés.

Dans le secteur public, ces risques sont particulièrement sensibles, car l'action administrative doit respecter les principes de légalité, d'égalité, de transparence et de responsabilité. Koppell (2005)⁶⁰ rappelle que la responsabilité publique est multidimensionnelle, puisqu'elle implique

⁵⁹ Janssen et Van Den Hoven, « Big and Open Linked Data (BOLD) in Government ».

⁶⁰ Koppell, « Pathologies of Accountability ».

à la fois la transparence, la conformité, la contrôlabilité, la réactivité et la responsabilité institutionnelle.

L'audit interne peut contribuer à la maîtrise de ces risques en évaluant la traçabilité des décisions numériques, la supervision humaine des traitements automatisés, la transparence des procédures et la clarté des responsabilités. Il peut également formuler des recommandations visant à renforcer les mécanismes de contrôle, à limiter les effets d'opacité et à garantir que les dispositifs numériques demeurent compatibles avec les principes fondamentaux du service public.

5.6. L'intégration des risques liés à la digitalisation dans la cartographie des risques

L'une des principales implications de la digitalisation pour l'audit interne réside dans la nécessité d'intégrer les risques liés à la digitalisation dans la cartographie globale des risques de l'organisation publique. Ces risques ne doivent pas être traités comme des risques périphériques, strictement informatiques ou isolés des processus métiers. Ils affectent simultanément les systèmes d'information, les données, les pratiques organisationnelles, les compétences des agents, l'accès des usagers aux services publics et les mécanismes de responsabilité institutionnelle.

La cartographie des risques doit donc permettre d'identifier les risques liés à la digitalisation, d'en apprécier la probabilité, l'impact et le niveau de maîtrise, mais aussi de mettre en évidence leurs interdépendances. Par exemple, une faiblesse dans la sécurité des systèmes d'information peut affecter la continuité du service public ; une mauvaise qualité des données peut fragiliser la fiabilité des décisions administratives ; une faible appropriation des outils par les agents peut réduire l'efficacité des dispositifs numériques ; une exclusion numérique peut remettre en cause l'égalité d'accès aux services publics.

Dans cette perspective, l'audit interne doit contribuer à faire évoluer la cartographie des risques en y intégrant des catégories spécifiques : risques technologiques et cybernétiques, risques liés aux données, risques organisationnels, risques humains et sociaux, risques éthiques et institutionnels. Cette intégration permet de mieux aligner les missions d'audit sur les transformations réelles des administrations publiques.

Conclusion

La digitalisation constitue aujourd'hui un levier structurant de modernisation du secteur public. En intégrant progressivement les technologies numériques dans les processus administratifs, elle contribue à améliorer l'efficacité des services, la traçabilité des opérations, la circulation de l'information et la qualité du service rendu à l'utilisateur. Toutefois, elle ne peut être réduite à une simple modernisation technique, car elle transforme également les modes de coordination, les responsabilités, les pratiques professionnelles et les mécanismes de contrôle au sein des administrations publiques.

L'analyse menée dans cet article montre que les risques liés à la digitalisation sont multidimensionnels. Ils ne se limitent pas aux risques numériques associés aux systèmes d'information, aux données et à la cybersécurité, mais englobent également des risques organisationnels, humains, sociaux, éthiques et institutionnels. La résistance au changement, l'exclusion numérique, les vulnérabilités liées aux données, l'opacité des traitements automatisés ou encore la complexification de la responsabilité publique illustrent cette diversité.

Dans ce contexte, la fonction d'audit interne est appelée à élargir son champ d'intervention afin d'intégrer les risques liés à la digitalisation dans ses missions d'assurance, de conseil et d'évaluation de la gouvernance. Cette évolution suppose leur prise en compte dans la cartographie globale des risques, le renforcement des compétences numériques des auditeurs, l'adaptation des méthodes d'audit aux environnements digitalisés et l'évaluation des dispositifs de cybersécurité, de gouvernance des données, d'inclusion numérique et de continuité du service public.

L'article met ainsi en évidence le rôle central de l'audit interne dans la maîtrise des risques liés à la digitalisation du secteur public. Au-delà de la vérification de conformité, il contribue à apprécier la robustesse des dispositifs numériques, la qualité des contrôles internes, l'appropriation des outils par les agents, l'accessibilité des services pour les usagers et la cohérence des choix de gouvernance.

Cette recherche présente toutefois une limite liée à sa nature théorique et conceptuelle. Des recherches futures pourraient la prolonger par des études de terrain, afin d'analyser concrètement la manière dont les fonctions d'audit interne intègrent ces risques dans leurs cartographies, leurs missions, leurs outils et leurs pratiques professionnelles.

Références bibliographiques

Abosson Koll, A., & Nneme Nneme, L. (2023). Comprendre la différence entre la transformation digitale et la digitalisation : Revue de la littérature pour un éclairage scientifique. *Revue Internationale du Chercheur*, 4(4), 665–674.

Armenakis, A. A., & Bedeian, A. G. (1999). Organizational change: A review of theory and research in the 1990s. *Journal of Management*, 25(3), 293–315. <https://doi.org/10.1177/014920639902500303>

Aubry, C., & Dufour, N. (2022). *Risk management : Organisation et positionnement de la fonction risk manager, méthodes de gestion des risques* (2e éd.). Gereso.

Bassrih, M. (2023). Management des risques inhérents à la transformation digitale des PME : Quel apport de l'audit interne ? *International Journal of Accounting, Finance, Auditing, Management & Economics*, 4(3-1), 183–196. <https://doi.org/10.5281/ZENODO.8023492>

Belaraj, A., & Oukassi, M. (2019). Qualité de l'audit interne au secteur public : Revue de la littérature. *Revue du Contrôle de la Comptabilité et de l'Audit*, 4(1), 672–697.

Belhaj, A., Salamate, F. E., Attar, H., & Zahi, J. (2025). La transformation digitale dans les organisations publiques marocaines : Nécessité ou effet de mode ? *Revue Economie & Kapital*, 1(27), 136–168.

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: Toward a next generation of insights. *MIS Quarterly*, 37(2), 471–482. <https://doi.org/10.25300/MISQ/2013/37:2.3>

Bonnet, D., & Rappin, B. (2023). *Résistance et résilience : Quel couplage ?* Institut Psychanalyse & Management.

Boudriga, Z. (2012). *Audit interne : Organisation et pratiques*. Azurite.

Brennen, J. S., & Kreiss, D. (2016). Digitalization. Dans K. B. Jensen & R. T. Craig (Éds.), *The international encyclopedia of communication theory and philosophy* (pp. 1–11). Wiley-Blackwell.

Bunting, C. (Éd.). (2008). *Global risk governance: Concept and practice using the IRGC framework* (Vol. 1, O. Renn & K. D. Walker, Éds.). Springer Netherlands. <https://doi.org/10.1007/978-1-4020-6799-0>

Chair, O., & Bounid, S. (2022). Transformation digitale des systèmes de gestion comme facteur de résilience organisationnelle : Revue de littérature. 5(3), 197–211.

Cordella, A., & Tempini, N. (2015). E-government and organizational change: Reappraising the role of ICT and bureaucracy in public service delivery. *Government Information Quarterly*, 32(3), 279–286. <https://doi.org/10.1016/j.giq.2015.03.005>

Djatkiko, G. H., Sinaga, O., & Pawirosumarto, S. (2025). Digital transformation and social inclusion in public services: A qualitative analysis of e-government adoption for marginalized communities in sustainable governance. *Sustainability*, 17(7), 2908. <https://doi.org/10.3390/su17072908>

Dunleavy, P., Margetts, H., Bastow, S., & Tinkler, J. (2006). *Digital era governance*. Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780199296194.001.0001>

El Yaacoubi, Y., & Bennani, H. (2021). Transformation digitale : Quelles reconfigurations pour les métiers de la banque de détail ? *Revue Internationale des Sciences de Gestion*, 5(1).

Fadili, M. H., & Ilahiane, N. (2022). Transition digitale ou transformation digitale : Revue de littérature pour éclairer la vision des PME et celle de leur écosystème. *International Journal of Accounting, Finance, Auditing, Management & Economics*, 3(5-1), 235–248.

Jacob, S., Defacqz, S., & Agossou, N. (2022). *Promesses et défis de la transformation numérique du secteur public* (Cahiers de recherche sur l'administration publique à l'ère numérique, no 6). Académie de la transformation numérique.

Janssen, M., & Van Den Hoven, J. (2015). Big and open linked data (BOLD) in government: A challenge to transparency and privacy? *Government Information Quarterly*, 32(4), 363–368. <https://doi.org/10.1016/j.giq.2015.11.007>

Koppell, J. G. S. (2005). Pathologies of accountability: ICANN and the challenge of "multiple accountabilities disorder." *Public Administration Review*, 65(1), 94–108. <https://doi.org/10.1111/j.1540-6210.2005.00434.x>

Kotter, J. (1996). *Leading change*. Harvard Business School Press.

Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation: Results from expert interviews. *Government Information Quarterly*, 36(4), 101385. <https://doi.org/10.1016/j.giq.2019.06.002>

Mesa, D. (2023). Digital divide, e-government and trust in public service: The key role of education. *Frontiers in Sociology*, 8, 1140416. <https://doi.org/10.3389/fsoc.2023.1140416>

O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown Publishing Group.

Ouhoud, O., & El Ouafa, K. (2025). Le rôle transformationnel de l'intelligence artificielle dans l'audit interne à l'ère du digital. *International Journal of Accounting, Finance, Auditing, Management & Economics*, 6(10), 560–578.

Parviainen, P., Tihinen, M., Kääriäinen, J., & Teppola, S. (2022). Tackling the digitalization challenge: How to benefit from digitalization in practice. *International Journal of Information Systems and Project Management*, 5(1), 63–77. <https://doi.org/10.12821/ijispm050104>

Power, M. (2004). The risk management of everything. *The Journal of Risk Finance*, 5(3), 58–65. <https://doi.org/10.1108/eb023001>

Renard, J., Nussbaumer, S., & Oriot, F. (2018). *Audit interne et contrôle de gestion : Pour une meilleure collaboration* (2e éd.). Eyrolles.

- Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, 23(15), 6666. <https://doi.org/10.3390/s23156666>
- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339. <https://doi.org/10.1016/j.jbusres.2019.07.039>
- Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society*, 71, 15–29. <https://doi.org/10.1016/j.aos.2018.04.005>
- Tilson, D., Lyytinen, K., & Sørensen, C. (2010). Research commentary — Digital infrastructures: The missing IS research agenda. *Information Systems Research*, 21(4), 748–759. <https://doi.org/10.1287/isre.1100.0318>
- Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management*, 14(3), 207–222. <https://doi.org/10.1111/1467-8551.00375>
- Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*, 122, 889–901. <https://doi.org/10.1016/j.jbusres.2019.09.022>
- Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, 28(2), 118–144. <https://doi.org/10.1016/j.jsis.2019.01.003>
- Volodina, T., & Grossi, G. (2025). Digital transformation in public sector auditing: Between hope and fear. *Public Management Review*, 27(5), 1444–1468. <https://doi.org/10.1080/14719037.2024.2402346>
- Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, 26(2), xiii–xxiii. <https://doi.org/10.2307/4132319>
- Wirtz, B. W., Daiser, P., & Binkowska, B. (2018). E-participation: A strategic framework. *International Journal of Public Administration*, 41(1), 1–12. <https://doi.org/10.1080/01900692.2016.1242620>

CHAPITRE 2 : *L'évaluation fondée sur le risque dans l'enseignement supérieur : principes, pratiques, comparaison internationale et proposition d'un modèle pour le Maroc*

Abdelali Kaaouachi, Université Mohammed Premier, Oujda ;

Mansour Serghini, Institut National de Recherche Halieutique, Casablanca

Pendant longtemps, l'assurance qualité dans l'enseignement supérieur a reposé sur des évaluations internes (par des cellules locales) et externes (par des agences et experts) conduites selon des cycles et des procédures largement uniformes. Conçu pour garantir l'équité de traitement, ce modèle a peu à peu montré ses limites à mesure que se diversifiaient les établissements, les modes de formation et les niveaux de risque.

Traiter tous les établissements de la même manière revient à ignorer leurs différences de gouvernance, de ressources et de performance académique. Cette uniformité retarde en outre l'identification des situations à risque et mobilise des ressources considérables, du côté des établissements comme des organismes d'évaluation.

L'évaluation fondée sur le risque (RBR) répond à ces limites en proportionnant la supervision au niveau de risque : les établissements dotés d'une gouvernance solide et affichant des résultats satisfaisants bénéficient d'un suivi allégé, tandis que ceux qui présentent des signaux d'alerte font l'objet d'une évaluation plus ciblée et plus rapprochée.

La RBR s'inscrit ainsi dans une gouvernance de la qualité plus proportionnée, réactive et efficiente. Ce chapitre en présente les fondements et les principes, les modalités de mise en œuvre, les principaux outils, ainsi qu'une typologie des risques universitaires. Il examine ensuite les expériences australienne, anglaise et américaine, avant de proposer un cadre d'adaptation au contexte marocain.

II. Signification de l'évaluation fondée sur le risque

L'évaluation fondée sur le risque consiste à moduler l'intensité, la fréquence et le périmètre de l'évaluation selon le niveau de risque identifié, au lieu d'appliquer un calendrier uniforme et une intervention exhaustive. Elle privilégie l'examen des situations qui cumulent une probabilité élevée de survenance et des conséquences significatives.

Elle peut être envisagée à deux niveaux. Au niveau externe, elle guide les organismes de régulation ou d'assurance qualité dans le choix des établissements à évaluer et dans la détermination de l'intensité du contrôle. Au niveau interne, elle aide les établissements à hiérarchiser leurs risques et à allouer leurs ressources en conséquence. Les deux dimensions se complètent : une gestion interne des risques jugée fiable ouvre la voie à une supervision externe plus proportionnée.

Là où l'évaluation cyclique suit un calendrier commun et où l'évaluation exhaustive prétend tout couvrir, la RBR opère une sélection des domaines et des établissements en fonction de leur profil de risque. Elle réduit la charge de contrôle pour les établissements les moins exposés et concentre la surveillance sur les situations qui appellent une attention particulière (Office for Students, 2018).

1. Le vocabulaire du risque

Le champ emprunte largement à la gestion des risques, et une poignée de termes reviennent tout au long de ce chapitre. Ils sont tirés de la norme internationale ISO 31000 (ISO, 2018) et du référentiel de gestion des risques d'entreprise du COSO (2017) :

- Risque : effet de l'incertitude sur les objectifs, entendu d'ordinaire comme la combinaison de la probabilité d'un événement et de la gravité de ses conséquences.
- Risque inhérent : niveau de risque avant tout contrôle ou mesure d'atténuation.
- Risque résiduel : niveau de risque qui subsiste une fois les contrôles en place ; c'est lui qui compte pour décider.
- Appétit pour le risque : quantité et nature de risque qu'un établissement accepte de prendre pour poursuivre ses objectifs.
- Contrôle : mesure qui réduit la probabilité ou l'impact d'un risque : politique, processus, audit, assurance.
- Probabilité et impact : les deux dimensions sur lesquelles le risque est coté, souvent croisées pour produire un score.
- Indicateur clé de risque (KRI) : signal mesurable annonçant qu'un niveau de risque évolue, idéalement assez tôt pour agir.
- Registre des risques : relevé central des risques identifiés, de leurs cotes, de leurs responsables, des contrôles en place et des actions prévues.

2. De la gestion des risques à l'évaluation fondée sur le risque

La gestion des risques s'est d'abord formalisée dans la finance, l'assurance, l'ingénierie et les grandes organisations, avant de gagner l'enseignement supérieur. Michael Power en a documenté l'expansion au cours des années 1990 et 2000, tout en mettant en garde contre une gestion du risque réduite à une démonstration formelle de contrôle, sans réelle diminution des risques (Power, 2004, 2007).

Cette évolution place les universités devant un double enjeu. Elles disposent désormais d'outils et de méthodes éprouvés, adaptables à leur contexte ; mais elles s'exposent aussi à une dérive documentaire, où la production de registres et de cartographies tient lieu de maîtrise effective des risques.

La RBR mobilise ces outils dans une perspective précise : déterminer où concentrer l'effort d'évaluation lorsque les ressources de contrôle sont limitées. Elle hiérarchise les risques et oriente l'attention vers ceux dont la probabilité et les conséquences potentielles pèsent le plus. En ce sens, elle constitue un mécanisme d'allocation rationnelle d'une ressource rare : l'attention évaluative.

III. Pourquoi les établissements et les régulateurs adoptent la RBR : les gains attendus

L'adoption de la RBR poursuit un double objectif : améliorer l'efficacité du contrôle et optimiser l'usage des ressources.

Pour les établissements, elle oriente l'attention de la gouvernance vers les risques susceptibles d'affecter le plus fortement leur mission. Un registre régulièrement actualisé facilite la hiérarchisation des risques, l'identification des responsabilités et le suivi des mesures correctives ; il favorise aussi la détection précoce des difficultés financières, académiques, organisationnelles ou technologiques. Une gestion interne efficace peut, de surcroît, renforcer l'autonomie de l'établissement en gagnant la confiance du régulateur.

Pour les régulateurs, la RBR autorise une supervision plus proportionnée : les ressources de contrôle vont en priorité aux établissements les plus exposés, plutôt que d'être réparties uniformément. Cette approche répond au principe selon lequel la régulation doit être guidée par le risque, la nécessité et la proportionnalité (TEQSA, 2019).

La RBR concourt également à la protection des étudiants et des deniers publics. Détecter tôt une fragilité financière ou institutionnelle laisse le temps de déployer des mesures préventives (plans de continuité en tête) avant que la situation ne devienne critique (U.S. Department of Education, 2023).

Elle peut enfin contenir les coûts de régulation dans un contexte d'expansion et de diversification de l'enseignement supérieur. Cette recherche d'efficacité ne saurait toutefois se réduire à une diminution des contrôles : l'efficacité du dispositif dépend de la qualité des données, des compétences d'analyse et de la justesse de l'appréciation des risques. La RBR ne consiste pas à contrôler moins, mais à contrôler mieux, au bon endroit et au bon moment.

IV. Principes méthodologiques

Une approche fondée sur le risque ne se résume pas à durcir le contrôle des situations jugées risquées. Elle repose sur quelques principes qui garantissent une évaluation cohérente, proportionnée et fondée sur des critères explicites.

La proportionnalité en constitue le principe central : l'intensité de l'évaluation doit être ajustée au niveau de risque. Les établissements peu exposés bénéficient d'un suivi allégé ; les plus exposés, d'une surveillance renforcée. Encore faut-il que l'appréciation des risques soit fiable.

Cette appréciation repose classiquement sur deux dimensions : la probabilité de survenue d'un événement défavorable et la gravité de ses conséquences. Leur combinaison hiérarchise les risques, mais le score global doit être lu comme un outil de classement, non comme une mesure exacte.

L'analyse doit privilégier le risque résiduel, celui qui subsiste après la mise en place des dispositifs de maîtrise. Deux établissements exposés à une même menace peuvent ainsi présenter des niveaux de risque résiduel très différents selon l'efficacité de leurs contrôles.

L'appétit pour le risque définit les niveaux de risque qu'un établissement accepte de prendre pour atteindre ses objectifs. Il distingue les risques inhérents à l'innovation et au développement de ceux qui demeurent difficilement acceptables (sécurité, intégrité, soutenabilité financière).

La surveillance continue vise à repérer rapidement les évolutions susceptibles de modifier le niveau de risque. Elle s'appuie sur des indicateurs, des données actualisées, les plaintes et signalements, ainsi que sur certains événements déclencheurs, faisant passer le dispositif d'une évaluation périodique à une veille dynamique.

Une gestion mature des risques suppose enfin une répartition claire des responsabilités, souvent structurée selon le modèle des « trois lignes » : la première assure la gestion quotidienne des risques, la deuxième définit les politiques et exerce la supervision, la troisième fournit une assurance indépendante, généralement par l'audit interne. Cette séparation renforce l'objectivité et la fiabilité du dispositif de maîtrise des risques.

V. Un modèle de mise en œuvre

La norme ISO 31000 propose un processus structuré de gestion des risques, aisément transposable à l'enseignement supérieur et aux dispositifs de régulation fondés sur le risque (ISO, 2018). Il peut se résumer en quelques étapes complémentaires :

- Établir le contexte : définir les objectifs, les résultats à protéger, l'appétit pour le risque et les critères d'appréciation. L'établissement part de sa mission et de sa stratégie ; le régulateur, de la protection des étudiants et de l'intérêt public.
- Identifier les risques : recenser les événements susceptibles d'entraver l'atteinte des objectifs, en mobilisant l'expérience des acteurs, les incidents passés et l'information sectorielle disponible. L'identification doit rester assez large pour ne pas écarter prématurément certains risques.
- Analyser et évaluer les risques : apprécier chaque risque selon sa probabilité et son impact, en tenant compte des dispositifs de maîtrise existants pour estimer le risque résiduel. Le registre et la cartographie facilitent la représentation et la hiérarchisation.
- Prioriser les risques : comparer les niveaux obtenus à l'appétit pour le risque. Ceux qui le dépassent appellent en général une action ; les autres peuvent être acceptés et suivis.
- Traiter les risques : renforcer les contrôles, transférer le risque, l'accepter ou, si nécessaire, mettre fin à l'activité concernée. Chaque mesure doit être associée à un responsable, une échéance et des critères de résultat.
- Surveiller et rendre compte : suivre régulièrement les indicateurs, les évolutions et les événements significatifs, afin d'actualiser l'appréciation des risques et d'informer les instances de gouvernance.
- Revoir et améliorer : évaluer périodiquement le dispositif pour vérifier la pertinence des risques identifiés, l'efficacité des mesures prises et la capacité du système à détecter des risques nouveaux.

Pour un régulateur, la démarche suit une logique analogue : définir les résultats à protéger, identifier les risques qui les menacent, les évaluer, cibler les interventions, suivre leur évolution et vérifier régulièrement l'efficacité du contrôle. Les expériences australienne et anglaise s'inscrivent dans cette logique, chacune selon des modalités propres à son contexte institutionnel.

VI. Outils et indicateurs

Les principes de la gestion des risques s'opérationnalisent à travers des outils relativement simples. Leur efficacité tient moins à leur sophistication qu'à la qualité des données, à la rigueur de leur usage et à la capacité de la gouvernance à agir sur les résultats.

1. Le registre, la matrice et la carte des risques

Le registre constitue l'outil central du dispositif. Pour chaque risque, il consigne la description, la probabilité, l'impact, le niveau de risque, les dispositifs de maîtrise existants, le risque résiduel, les responsables, les actions prévues et leur avancement. Pour rester utile, il doit demeurer synthétique, actualisé et orienté vers la décision ; trop volumineux, il dilue l'attention portée aux risques réellement critiques.

La matrice probabilité-impact, souvent construite sur cinq niveaux, permet de visualiser et de hiérarchiser les principaux risques ; elle facilite la communication avec les instances de gouvernance et fait ressortir d'un coup d'œil les priorités. La carte des risques doit néanmoins être maniée comme un outil d'aide à la décision, non comme une mesure exacte : les niveaux attribués reposent en partie sur des appréciations et peuvent suggérer une précision supérieure à la réalité.

Probabilité \ Impact	Mineur	Modéré	Majeur	Grave
Quasi certaine	Moyen	Élevé	Extrême	Extrême
Probable	Moyen	Élevé	Élevé	Extrême
Possible	Faible	Moyen	Élevé	Élevé
Peu probable	Faible	Faible	Moyen	Élevé
Rare	Faible	Faible	Moyen	Moyen

Tableau 1 : Une grille type probabilité × impact.

2. Indicateurs clés de risque, scores composites, tableaux de bord et échelles de maturité

Les indicateurs clés de risque (KRI) servent à détecter les évolutions annonciatrices d'une matérialisation du risque. Pour être pertinents, ils doivent être mesurables, régulièrement disponibles et directement liés au risque suivi ; ils portent typiquement sur la situation financière, les performances académiques, la satisfaction des étudiants ou les ressources humaines.

Tout l'enjeu consiste à retenir un nombre limité d'indicateurs capables de fournir des signaux suffisamment précoces : un indicateur qui ne réagit qu'après la survenue du problème relève du constat, non de l'alerte. Les régulateurs développent d'ailleurs leurs propres indicateurs à partir des données relatives aux étudiants, au personnel, aux finances, aux plaintes et aux événements déclarables.

Les scores composites synthétisent plusieurs indicateurs en une valeur unique, commode pour la communication et la comparaison, mais susceptible de masquer les facteurs à l'origine du résultat. Les tableaux de bord offrent une alternative en conservant la visibilité sur chaque indicateur et son évolution.

Les échelles de maturité mesurent, quant à elles, le degré de développement de la capacité d'un établissement à gérer ses risques (d'une approche essentiellement réactive à un système intégré d'amélioration continue). Elles rappellent qu'une gestion efficace des risques ne se réduit pas à leur identification et à leur notation : elle suppose le développement progressif des capacités institutionnelles nécessaires à leur maîtrise.

VII. Une typologie des risques dans l'enseignement supérieur

Les établissements d'enseignement supérieur sont des organisations complexes, avec une variété de missions : enseignement, recherche, innovation et service à la société, tout en mobilisant des ressources humaines et financières importantes, en gérant des infrastructures et des données sensibles, et en devant préserver leur réputation comme leur intégrité académique.

Cette diversité de missions et de ressources engendre un large éventail de risques, souvent interdépendants et relevant parfois de plusieurs catégories à la fois. La typologie ci-dessous offre un cadre de référence pour structurer leur identification, leur analyse et leur suivi.

Catégorie de risque	Ce qu'elle couvre	Signes d'alerte typiques
Gouvernance et stratégie	Décisions faibles ou en conflit d'intérêts ; responsabilités floues ; stratégie déconnectée du réel ; faible supervision du conseil.	Individus dominants ; constats d'audit non résolus ; forte rotation au sommet ; décisions sans traces.
Qualité et standards académiques	Standards non tenus ; mauvais résultats étudiants ; offre désalignée ou périmée ; intégrité de l'évaluation.	Baisse de la poursuite et de la réussite ; remarques des examinateurs externes ; inflation des notes ; plaintes en hausse.
Financier	Insolvabilité ; dépendance à une source de revenu ; base de coûts insoutenable ; placements ratés.	Liquidité en baisse ; déficits de recrutement ; budgets déficitaires ; concentration sur un marché.
Conformité et réglementation	Manquement aux conditions, à la loi ou aux règles de financement ; perte d'accréditation ou du droit de délivrer des diplômes.	Reporting manqué ; constats défavorables ; changements qui violent les conditions ; questions du régulateur.
Personnes et ressources humaines	Incapacité à recruter ou retenir des profils clés ; conflit social ; lacunes de compétences ; surcharge et mal-être.	Vacances et rotation dans les rôles critiques ; griefs ; dépendance à quelques individus ; signaux d'épuisement.
Cybersécurité et données	Violation ou perte de données personnelles et de recherche ; rançongiciel ; panne ; non-conformité à la vie privée.	Hameçonnage réussi ; systèmes non corrigés ; pas de plan de reprise testé ; incidents évités de justesse.
Réputation	Perte de confiance des étudiants, du personnel, des partenaires et du public, méritée ou provoquée par les événements.	Couverture négative ; baisse dans les enquêtes ; retrait de partenaires ; incidents mal gérés.

Catégorie de risque	Ce qu'elle couvre	Signes d'alerte typiques
Intégrité de la recherche et éthique	Inconduite ; manquements à l'éthique ou à la sécurité ; conflits d'intérêts ; détournement de fonds.	Allégations ; rétractations ; revue éthique faible ; constats d'audit sur les financements.
Patrimoine, infrastructures, sécurité	Défaillance de bâtiments, d'équipements ou de systèmes de sécurité ; maintenance différée ; dangers physiques.	Arriéré de maintenance ; incidents de sécurité ; actifs critiques vieillissants ; inspections ratées.
Chocs externes et stratégiques	Changement de politique ; visas et immigration ; perturbation de marché ou géopolitique ; pandémies.	Réformes annoncées ; règles de visa modifiées ; déplacements de la demande ; tensions sectorielles.

Tableau 2 : Typologie des risques en milieu universitaire.

VIII. Comparaison internationale des modèles

La comparaison porte sur trois systèmes nationaux d'évaluation fondée sur le risque : l'Australie, l'Angleterre et les États-Unis. Ils méritent d'être étudiés ensemble parce qu'ils résolvent le même problème de manières nettement différentes.

1. Australie : une appréciation annuelle structurée

L'Australie figure parmi les précurseurs de la régulation fondée sur le risque, depuis la création de la Tertiary Education Quality and Standards Agency (TEQSA) en 2011. Son cadre repose sur trois principes : le risque, la nécessité et la proportionnalité, qui ajustent l'intensité des interventions au profil de chaque établissement.

TEQSA conduit une appréciation annuelle des établissements enregistrés, adossée au Higher Education Standards Framework. L'analyse couvre plusieurs dimensions : effectifs et résultats des étudiants, expérience étudiante, ressources humaines, situation financière. Elle exploite les données relatives aux étudiants, au personnel et aux comptes audités afin de repérer les établissements requérant une attention particulière (TEQSA, 2015).

Le modèle australien ne supprime donc pas l'évaluation régulière : il en différencie l'intensité. Les établissements au profil de risque faible bénéficient d'une supervision allégée et d'une autonomie accrue ; les situations vulnérables font l'objet d'interventions approfondies.

Cette approche a progressivement renforcé la logique d'auto-assurance (self-assurance), en incitant les établissements à développer leurs propres dispositifs de gouvernance et de gestion des risques (Gallagher, 2012). Elle cible mieux les ressources de régulation et favorise une détection plus précoce des difficultés, tout en soulevant des questions sur la fiabilité des indicateurs, l'interprétation des données et l'équilibre entre supervision réglementaire et autonomie institutionnelle.

L'expérience australienne illustre ainsi un principe essentiel de la RBR : une surveillance générale fondée sur les données, couplée à une intervention proportionnée au niveau de risque.

2. Angleterre : une régulation dynamique et fondée sur les données

L'Angleterre a développé son approche fondée sur le risque à partir des années 2010, d'abord avec le Higher Education Funding Council for England (HEFCE) et la Quality Assurance Agency (QAA), puis avec la création de l'Office for Students (OfS) en 2018, dans le cadre du Higher Education and Research Act 2017. L'objectif : substituer aux contrôles institutionnels uniformes une supervision proportionnée, tenant compte du profil de risque et de l'historique de conformité de chaque établissement (Jackson, 2015).

Le modèle actuel repose sur une surveillance continue, assise sur des conditions permanentes d'enregistrement et sur l'analyse régulière des données disponibles. L'OfS actualise son appréciation du risque au fil des informations nouvelles : indicateurs de performance, plaintes, signalements, événements déclarables. Lorsqu'un risque de manquement se dessine, une intervention peut être engagée pour en vérifier la réalité et, le cas échéant, prendre les mesures appropriées (Office for Students, 2018).

Cette approche accélère l'intervention et améliore l'allocation des ressources de régulation. Elle accorde aussi un poids important à la gouvernance : une faiblesse dans la gestion d'un risque peut signaler des vulnérabilités plus larges.

La forte dépendance aux données comporte cependant des limites (King, 2015) : les indicateurs peuvent manquer certains risques émergents ou qualitatifs, en particulier lorsqu'ils ne se mesurent pas directement. Des contrôles complémentaires (vérifications ciblées ou aléatoires) demeurent nécessaires pour limiter les angles morts.

L'expérience anglaise illustre ainsi une forme avancée de la RBR : une surveillance continue, largement fondée sur les données, complétée par des interventions ciblées dès que des signaux de risque apparaissent.

3. États-Unis : une approche centrée sur le risque financier

Aux États-Unis, l'assurance qualité repose sur une « Triade » associant le gouvernement fédéral, les États et les organismes d'accréditation. Dans ce système décentralisé, les approches fondées sur le risque sont venues compléter les dispositifs traditionnels de réaccréditation périodique.

Le modèle américain fait une place centrale aux risques financiers, en raison du volume des financements fédéraux destinés aux étudiants et de la nécessité de protéger les fonds publics. Le U.S. Department of Education calcule un score composite de responsabilité financière à partir de plusieurs ratios ; le niveau obtenu peut déterminer l'intensité du suivi et les conditions d'accès aux financements fédéraux (U.S. Department of Education, 2019).

Les établissements financièrement fragiles peuvent ainsi être placés sous contrôle renforcé, en particulier à travers des mécanismes de surveillance des flux liés à l'aide fédérale. Les interventions se concentrent sur les situations les plus risquées, tandis que les contrôles supplémentaires s'allègent pour les établissements jugés sains.

Parallèlement, certaines agences d'accréditation modulent leur suivi à partir d'indicateurs de persévérance, de résultats étudiants, de performance financière ou d'autres dimensions institutionnelles.

Le modèle présente toutefois une limite notable : une focalisation marquée sur les indicateurs quantitatifs et financiers peut donner une vision partielle de la qualité universitaire et sous-estimer la diversité des missions, les contextes institutionnels et les dimensions qualitatives qu'apprécie l'évaluation par les pairs.

L'expérience américaine illustre ainsi une RBR particulièrement aboutie dans le champ financier : un indicateur mesurable de fragilité peut déclencher automatiquement un niveau de surveillance supérieur, au service de la protection des étudiants et des fonds publics.

4. Ce que la comparaison montre

Mis côte à côte, les trois systèmes diffèrent par l'universalité de l'appréciation, sa fréquence, son objet et la portée de ses conséquences.

Caractéristique	Australie (TEQSA)	Angleterre (OfS)	États-Unis (ED)
Couverture	Chaque établissement, chaque année	Risque apprécié à l'enregistrement, puis ciblé	Tous les établissements aidés
Rythme	Cycle annuel	Continu, sans cycle fixe	Dépôt financier annuel, avec déclencheurs
Objet principal	Risque pour les étudiants et les finances	Risque de manquement aux conditions	Responsabilité financière
Colonne vertébrale	ISO 31000 ; cadre de standards	Principes et conditions d'enregistrement	Score composite de ratios comptables
Déclencheur d'action	Note de risque élevée	Risque accru de manquement ; événements déclarables	Score sous le seuil
Conséquence la plus forte	Contrôle réglementaire intensifié	Sanction en cas de manquement avéré	Contrôle de trésorerie et lettre de crédit

Tableau 3 : Trois modèles nationaux comparés.

Les trois expériences convergent sur un principe central : concentrer l'effort de contrôle sur les établissements et les situations les plus à risque, au premier chef pour les étudiants et les finances publiques. Toutes accordent une place importante à la soutenabilité financière et cherchent à alléger la charge réglementaire des établissements peu exposés.

Elles se distinguent en revanche par l'équilibre retenu entre couverture, réactivité et intensité du contrôle. L'Australie maintient une appréciation régulière de tous les établissements, en modulant l'intensité des interventions ; l'Angleterre privilégie une surveillance continue, déclenchée par l'évolution des données et des signaux de risque ; les États-Unis donnent la primauté au risque financier, avec des mécanismes pouvant entraîner automatiquement un contrôle renforcé (NCHEMS, 2017).

Il n'existe donc pas de modèle unique de la RBR. Le choix dépend du niveau de maturité du système, de la qualité des données disponibles et des capacités du régulateur. Pour un système en phase de développement, une appréciation régulière et universelle, à l'australienne, peut constituer une étape prudente avant d'évoluer vers une surveillance plus dynamique ; à mesure que données et capacités d'analyse se renforcent, certains mécanismes du modèle anglais peuvent être intégrés. L'expérience américaine, elle, enseigne l'intérêt de seuils de risque explicites associés à des mesures de contrôle proportionnées.

L'enjeu n'est pas de reproduire un modèle existant, mais de construire un dispositif adapté au contexte institutionnel, aux données disponibles et aux capacités nationales de régulation.

IX. La méthode appliquée : deux illustrations

Les principes et les outils de la RBR se déclinent à différents niveaux, selon les responsabilités de l'acteur concerné. Deux exemples l'illustrent, à l'échelle d'un établissement puis d'un régulateur.

1. Au niveau d'un établissement : la revue du portefeuille de programmes

Une université soumettait ses programmes à une évaluation complète selon un cycle uniforme de six ans, quelle que soit leur situation. Elle a remplacé ce dispositif par une revue de portefeuille fondée sur le risque, articulée autour de quelques indicateurs : évolution des effectifs, poursuite et réussite, satisfaction des étudiants, observations des examinateurs externes, devenir des diplômés.

Les programmes à faible risque font désormais l'objet d'un suivi annuel allégé et d'une évaluation approfondie tous les six ans ; ceux qui présentent des signaux d'alerte, d'une revue ciblée et rapprochée. La charge globale d'évaluation diminue, tandis que les ressources se concentrent sur les situations qui appellent une intervention.

2. Au niveau du régulateur : la détection précoce d'une fragilité

Un régulateur peut également exploiter des indicateurs suivis régulièrement pour repérer les signes de fragilité d'un établissement. Une liquidité qui s'érode, des retards de reporting, des plaintes en hausse : pris isolément, ces signaux peuvent sembler insuffisants ; leur évolution combinée peut en revanche révéler une situation préoccupante.

La montée du niveau de risque déclenche alors une analyse approfondie, un échange avec la gouvernance et, le cas échéant, un plan de continuité. Une intervention précoce limite les conséquences pour les étudiants et permet, si nécessaire, d'organiser une transition ordonnée.

Ces deux exemples le montrent : la RBR ne vise pas à multiplier les contrôles, mais à détecter plus tôt les situations préoccupantes et à concentrer les ressources là où elles produisent le plus

d'effet. Son efficacité reste suspendue à la fiabilité des données, à leur disponibilité en temps utile et à la qualité du jugement porté sur leur évolution.

X. Avantages, limites et conditions de réussite

La RBR présente un intérêt majeur pour l'enseignement supérieur, mais son efficacité dépend étroitement de la qualité de sa conception et de sa mise en œuvre.

Ses avantages sont réels. Elle permet une allocation plus efficiente des ressources de contrôle, concentrées sur les établissements, domaines ou activités les plus exposés ; les établissements à faible risque voient leur charge administrative diminuer sans que l'assurance qualité en pâtisse. Elle améliore la réactivité de la régulation : le suivi régulier des indicateurs et des événements significatifs aide à détecter les difficultés (financières, académiques, organisationnelles) avant qu'elles ne deviennent critiques, au bénéfice des étudiants et des ressources publiques. En interne, enfin, elle renforce la gouvernance et le pilotage en aidant les instances dirigeantes à hiérarchiser les risques et à orienter les ressources vers les priorités institutionnelles.

Ses limites ne le sont pas moins. La première tient à la difficulté de prévoir : certains événements majeurs sont par nature imprévisibles ou échappent aux indicateurs disponibles, et la RBR ne saurait garantir l'identification de tous les risques. La deuxième concerne la qualité et l'usage des données : dès lors que les indicateurs emportent des conséquences réglementaires, les établissements peuvent être tentés d'optimiser leur performance apparente plutôt que la réalité sous-jacente ; c'est la loi de Goodhart : lorsqu'une mesure devient une cible, elle cesse d'être une bonne mesure (Strathern, 1997). La troisième réside dans le risque de complaisance envers les établissements réputés peu risqués : une notation favorable ne doit pas se traduire par une absence durable de contrôle, et des vérifications ponctuelles ou aléatoires restent nécessaires pour débusquer ce que les indicateurs ne voient pas. La RBR peut enfin survaloriser le mesurable : les données financières ou de résultats étudiants s'exploitent aisément, quand l'érosion de la culture académique, les atteintes à l'intégrité ou les fragilités de gouvernance se quantifient mal.

La réussite du dispositif suppose plusieurs conditions. Des données fiables, actualisées et suffisamment diversifiées d'abord, complétées par une analyse qualitative qui en éclaire la signification. Une gouvernance indépendante ensuite, capable de questionner les appréciations de risque, et un appétit pour le risque clairement défini. L'évaluation, par ailleurs, n'a de valeur que si elle débouche sur des décisions : chaque risque identifié doit être associé à des responsables, des actions et des mécanismes de suivi. Le dispositif doit enfin intégrer une marge d'incertitude et des contrôles complémentaires (revues ciblées, contrôles aléatoires, tests de résistance). La RBR ne doit pas être conçue comme un système prédictif parfait, mais comme un cadre qui oriente mieux l'attention, détecte plus tôt les signaux de fragilité et permet d'agir de manière proportionnée.

XI. Recommandations pour la mise en place d'une évaluation fondée sur le risque

La mise en place d'une RBR doit être progressive, adaptée au contexte et orientée vers la décision. Dix recommandations s'en dégagent :

- Partir des objectifs institutionnels : identifier ce que l'établissement ou le système cherche à atteindre et à protéger avant de définir les risques, sans reproduire mécaniquement un modèle externe.
- Privilégier la simplicité : limiter le registre aux risques réellement significatifs et retenir un petit nombre d'indicateurs pertinents et précoces.
- Évaluer le risque résiduel et définir l'appétit pour le risque : apprécier les risques après prise en compte des dispositifs de maîtrise et préciser les niveaux acceptables.
- Investir dans la qualité des données : s'assurer de données fiables, actualisées et accessibles avant de fonder les décisions sur des scores de risque.
- Garantir une appréciation indépendante : permettre la remise en question des évaluations et préserver l'indépendance des fonctions d'assurance et d'audit.
- Relier l'évaluation à l'action : associer chaque risque important à un responsable, des mesures, des échéances et des résultats attendus, puis vérifier leur efficacité.
- Prévoir la détection des angles morts : compléter les indicateurs par des contrôles aléatoires, des analyses de scénarios et des tests de résistance.
- Déployer progressivement : dans un système peu mature, commencer par une appréciation générale et légère, puis évoluer vers une surveillance plus continue et ciblée quand les données et les compétences le permettent.
- Gérer la réputation par la maîtrise des risques : la considérer comme la conséquence de la qualité de la gouvernance, de la prévention et de la gestion des incidents, plutôt que comme un risque isolé.
- Évaluer régulièrement le dispositif lui-même : vérifier périodiquement sa capacité à détecter les risques pertinents et à améliorer effectivement les décisions. Une RBR doit rester un système d'apprentissage et d'amélioration continue.

XII. Proposition d'un modèle marocain d'évaluation fondée sur le risque

Le Maroc pourrait introduire progressivement la RBR dans l'enseignement supérieur sans transposer tel quel un modèle étranger. Compte tenu de la maturité actuelle des données et des capacités d'analyse, une approche hybride et progressive paraît la plus adaptée : maintenir une évaluation légère de l'ensemble des établissements, tout en renforçant le contrôle des situations à risque élevé.

1. Un contexte favorable

Les réformes engagées créent un terrain propice à cette évolution. La loi-cadre n° 51-17 et les orientations du Nouveau Modèle de Développement placent la gouvernance, la qualité, la responsabilité et l'autonomie au cœur de la transformation du système.

Or l'autonomie institutionnelle appelle une contrepartie : l'État doit pouvoir s'assurer de la qualité et de la soutenabilité du système sans recourir à un contrôle uniforme et permanent. C'est précisément ce que permet la RBR, en articulant autonomie, responsabilité et supervision proportionnée.

Plusieurs atouts facilitent son introduction au Maroc : l'existence de l'Agence nationale d'évaluation et d'assurance qualité de l'enseignement supérieur et de la recherche scientifique (ANEAQ), qui offre une base institutionnelle au dispositif ; la progression de la digitalisation et des systèmes d'information, indispensables à une régulation fondée sur les données ; la diversité croissante du paysage (établissements publics, privés et partenariats) qui justifie une différenciation des modalités de contrôle.

2. Principes de conception d'un modèle marocain

Le modèle marocain gagnerait à reposer sur quelques principes structurants :

- adapter plutôt qu'importer, en s'appuyant sur le référentiel national de l'ANEAQ et les standards internationaux ;
- commencer par une couverture universelle légère, puis renforcer progressivement le ciblage à mesure que s'améliorent la qualité des données et les capacités d'analyse ;
- combiner risque et évaluation périodique, afin qu'aucun établissement réputé peu risqué ne soit durablement soustrait à toute évaluation approfondie ;
- renforcer l'autonomie responsable, en allégeant la charge externe des établissements dotés de dispositifs internes de qualité et de gestion des risques performants ;
- couvrir l'ensemble du secteur, avec une intensité de contrôle proportionnée au risque ;
- garantir la transparence sur les critères, les indicateurs et les modalités de calcul des profils de risque.

3. Un modèle marocain à deux niveaux

Le dispositif pourrait s'articuler autour de deux niveaux complémentaires.

Le premier niveau prendrait la forme d'un profil de risque institutionnel annuel. Chaque établissement ferait l'objet d'un criblage léger, réalisé pour l'essentiel sur pièces à partir des données des systèmes d'information. Ce criblage identifierait les principaux signaux de risque et classerait les établissements par niveaux de vigilance, sans mobiliser systématiquement des visites ou des procédures lourdes.

Le second niveau consisterait en une évaluation approfondie ciblée. Une évaluation complète (auto-évaluation, expertise externe et, si nécessaire, visite sur site) serait déclenchée en priorité pour les établissements présentant des signaux de risque élevés. Elle demeurerait obligatoire, à intervalles réguliers, pour tous les établissements, y compris les moins exposés.

Le dispositif combinerait ainsi surveillance continue et évaluation de référence : intervenir vite lorsqu'un risque apparaît, tout en conservant une garantie minimale d'évaluation pour l'ensemble du système. Sa crédibilité tiendra à la qualité du profil de risque institutionnel, qui devrait reposer sur un nombre limité d'indicateurs fiables, comparables et réellement disponibles : une dizaine d'indicateurs robustes et régulièrement renseignés vaudra toujours mieux qu'un dispositif complexe fondé sur des données incomplètes.

Deux éléments conditionnent la crédibilité du modèle. D'abord, l'évaluation devrait porter sur le risque résiduel (le niveau de risque après prise en compte des dispositifs de maîtrise) de façon à valoriser les établissements qui démontrent une capacité réelle de prévention et de maîtrise.

Ensuite, le dispositif devrait s'adosser à un appétit national pour le risque, précisant les domaines de tolérance minimale : soutenabilité financière, intégrité académique et scientifique, sécurité des étudiants, etc. Ces deux garde-fous évitent de réduire la RBR à un simple classement statistique.

La matrice d'autonomie méritée

Le modèle à deux niveaux dit quand renforcer l'évaluation ; il doit aussi dire quand l'alléger. La logique d'« autonomie méritée » répond à cette question.

L'intensité du contrôle serait déterminée par deux dimensions complémentaires : le niveau de risque résiduel de l'établissement, d'une part ; la maturité et la fiabilité de ses systèmes internes de qualité et de gestion des risques, d'autre part.

Un faible niveau de risque ne suffirait donc pas, à lui seul, à justifier un allègement notable du contrôle : encore faut-il que l'établissement démontre une capacité fiable à identifier, maîtriser et signaler ses risques.

La RBR devient ainsi un levier d'autonomie responsable : plus un établissement prouve sa capacité à se gouverner et à maîtriser ses risques, plus la supervision externe peut s'alléger.

Risque / Maturité QA interne	Émergente	En développement	Établie
Élevé	Renforcé : évaluation complète à cycle court, accompagnement rapproché, montée en capacité	Intensif : évaluation complète, plan d'action requis et suivi	Intensif mais collaboratif : évaluation complète, en s'appuyant sur la remédiation propre de l'établissement
Modéré	Renforcé : évaluation ciblée, surveillance et accompagnement rapprochés	Standard renforcé : évaluation ciblée du domaine signalé, surveillance	Ciblé : évaluation ciblée du domaine signalé ; confiance aux contrôles internes ailleurs
Faible	Standard : profil annuel et cycle de référence, avec appui à la montée en maturité	Standard : profil annuel et cycle de référence	Autonomie méritée : profil annuel seul ; évaluation de référence à l'intervalle le plus long

Tableau 4 : La matrice d'autonomie méritée.

La matrice traduit ce principe en règle opérationnelle, en croisant le niveau de risque de l'établissement et la maturité de ses systèmes internes. Les établissements à faible risque dotés de dispositifs matures bénéficient d'une supervision allégée ; ceux dont les risques sont élevés

ou dont les systèmes internes restent embryonnaires appellent un contrôle plus étroit, éventuellement assorti d'un appui au renforcement des capacités.

Cette approche évite d'accorder une autonomie accrue sur la seule foi de résultats favorables : un faible risque doit être confirmé par une capacité institutionnelle démontrée à le maîtriser. La matrice devient dès lors un outil de différenciation progressive de la supervision et un mécanisme d'incitation à l'amélioration des systèmes internes.

L'objectif ultime est de permettre aux établissements de progresser vers une autonomie méritée, fondée à la fois sur la maîtrise des risques et sur la maturité de leur gouvernance et de leur assurance qualité.

4. Gouvernance et pilotage du dispositif

Un système d'évaluation fondé sur le risque exige une gouvernance claire, qui distingue la définition des orientations, la mise en œuvre opérationnelle et l'assurance indépendante. Une architecture à trois niveaux peut être envisagée, avec l'ANEAQ en acteur opérationnel central.

i) *Un comité national de pilotage.* Cette instance définirait les orientations du dispositif, approuverait les indicateurs et les seuils de risque et suivrait sa performance. Elle réunirait le ministère chargé de l'enseignement supérieur, l'ANEAQ, des représentants des universités, des experts indépendants ainsi que des représentants des étudiants et du monde socio-économique. Son rôle serait stratégique, non opérationnel.

ii) *L'ANEAQ, chef de file opérationnel.* L'agence assurerait la mise en œuvre : collecte et validation des données, établissement des profils annuels de risque, déclenchement et conduite des évaluations approfondies. Une unité spécialisée d'analyse des risques et des données, distincte des équipes d'évaluation, garantirait la robustesse de la méthodologie et l'exploitation des informations.

iii) *Une propriété institutionnelle des risques.* Chaque établissement disposerait d'une fonction de pilotage des risques, appuyée sur une instance interne et chargée de l'identification des risques, de leur suivi et de la fiabilité des données transmises. Cette responsabilité interne conditionne l'autonomie responsable.

La séparation des fonctions est déterminante : l'instance qui définit les règles ne devrait pas être chargée de leur application, et les établissements ne devraient pas être seuls juges de la qualité des données qu'ils produisent. Des mécanismes d'assurance indépendante (audit interne, évaluation périodique du dispositif de l'ANEAQ) complèteraient l'architecture, garantissant à la fois cohérence nationale, indépendance, responsabilité institutionnelle et crédibilité.

Fonction	Comité de pilotage	ANEAQ	Établissement
Fixer la politique, les indicateurs, les seuils	Approuve	Propose	Consulté

Fonction	Comité de pilotage	ANEAQ	Établissement
Collecter et valider les données	Supervise	Exécute	Soumet
Produire le profil de risque annuel	Examine	Produit	Reçoit, peut contester
Conduire l'évaluation approfondie	Supervise	Conduit	S'auto-évalue, accueille
Gérer le risque interne	—	Appuie	Possède
Évaluer le système lui-même	Commande	Rend compte	Donne son retour

Tableau 5 : Répartition des responsabilités.

5. Feuille de route de mise en œuvre

Une mise en œuvre par phases permet au modèle de gagner la confiance en chemin, en plaçant d'abord le prérequis le plus ingrat : les données.

Phase	Objet	Principaux livrables
0. Préparation	Mandat et fondations	Base juridique par la loi réformée de l'ANEAQ ; infrastructure de données rendue possible par la refonte des SI ; jeu d'indicateurs et seuils définis ; analystes formés.
1. Pilote	Tester et calibrer	Pilote avec des établissements volontaires ; validation des indicateurs face au réel ; calibrage des seuils ; leçons réinjectées dans la méthode.
2. Criblage universel	Déployer le niveau 1	Profils de risque annuels pour tous les établissements publics, privés et en partenariat ; méthodologie publiée ; profils partagés avec chaque établissement.
3. Évaluation déclenchée	Activer le niveau 2	Évaluations approfondies déclenchées par le risque, aux côtés d'un cycle de référence ; intégration aux décisions d'accréditation ; suivi allégé pour les établissements à forte gestion interne.
4. Maturité	Affiner vers la réactivité	À mesure que les données se révèlent fiables, allongement des cycles de référence des établissements à faible risque et recours accru à la

Phase	Objet	Principaux livrables
		surveillance continue ; méta-évaluation périodique du système.

Tableau 6 : Une mise en œuvre par phases.

La transition vers une régulation plus ciblée doit rester progressive et fondée sur des preuves. Le passage d'un criblage universel à une surveillance principalement fondée sur le risque ne devrait intervenir qu'une fois démontrées la fiabilité des données, la pertinence des indicateurs et la capacité effective du dispositif à détecter les situations à risque.

Pour un système encore en développement, maintenir une évaluation légère de l'ensemble des établissements constitue une garantie importante : y renoncer trop tôt réduirait la capacité de détection au lieu de renforcer l'efficacité. L'évolution vers une RBR plus mature doit donc se concevoir comme une étape à gagner, conditionnée par la qualité des données, la maturité des capacités d'analyse et l'efficacité démontrée de la surveillance.

6. Suivi et évaluation du dispositif

Un système d'évaluation fondé sur le risque doit lui-même être évalué régulièrement et de manière critique. L'enjeu n'est pas seulement de vérifier la conformité des établissements, mais de déterminer si le dispositif détecte effectivement les risques qu'il est censé identifier.

Sa performance peut être suivie à travers des indicateurs portant sur la capacité de détection, la réactivité, la pertinence des alertes et l'efficacité des interventions : complétude et ponctualité des données (données arrivant à temps pour agir) ; couverture (tous les établissements profilés chaque année) ; délai de détection (fragilité signalée avant qu'elle ne nuise aux étudiants) ; taux de confirmation des cas signalés (la plupart des alertes orange et rouges confirmées à l'examen) ; vérification des risques manqués (peu de surprises lors des tirages aléatoires de cas à faible risque) ; charge (les établissements à suivi allégé déclarent une charge faible) ; clôture des actions (la plupart des actions requises achevées et vérifiées) ; confiance des parties prenantes (établissements et public jugent le dispositif juste et utile).

Trois mécanismes renforcent la fiabilité de l'ensemble : les contrôles aléatoires d'établissements à faible risque, pour débusquer les angles morts ; la révision annuelle des indicateurs et des seuils, pour suivre l'évolution des risques et des comportements institutionnels ; l'évaluation indépendante périodique du dispositif, incluant, le cas échéant, une revue externe de l'ANEAQ selon les standards internationaux. Ainsi la RBR reste-t-elle pertinente, objective et capable de détecter les risques émergents.

7. Conditions et réserves pour le cas marocain

La mise en œuvre de la RBR au Maroc est prometteuse, mais elle demeure conditionnée à plusieurs facteurs. La fiabilité des données constitue le premier prérequis, suivie du développement des compétences en analyse des risques et en évaluation. Il faut aussi éviter que la gestion documentaire ne se substitue à la maîtrise effective des risques.

Deux autres enjeux sont essentiels : préserver l'équilibre entre régulation nationale et autonomie institutionnelle, et prévenir le pilotage stratégique des indicateurs par les établissements lorsque ceux-ci conditionnent le niveau de contrôle.

Ces réserves n'invalident pas la démarche ; elles plaident pour une mise en œuvre progressive : renforcer d'abord les données et les capacités, maintenir une couverture universelle légère, puis développer le ciblage par le risque, tout en évaluant régulièrement le dispositif lui-même.

Conclusion

L'évaluation fondée sur le risque marque une rupture avec le contrôle uniforme : elle concentre les ressources de supervision là où les risques sont les plus élevés. Les expériences australienne, anglaise et américaine en montrent des déclinaisons différentes, mais convergentes dans leur recherche de proportionnalité, de réactivité et d'efficacité.

Pour le Maroc, la réforme vers une autonomie universitaire responsable offre un contexte favorable à un modèle hybride : une surveillance légère de l'ensemble du secteur, complétée par des évaluations approfondies lorsque les indicateurs le justifient. La matrice d'autonomie méritée lierait progressivement l'allègement du contrôle au faible niveau de risque comme à la maturité des dispositifs internes de qualité et de gestion des risques.

L'approche est exigeante : elle suppose des données fiables, des compétences d'analyse, une véritable indépendance et une capacité d'intervention, ainsi que des contrôles aléatoires et une révision régulière des indicateurs pour limiter ses propres angles morts.

Au final, la performance d'un système RBR ne se mesure pas à la sophistication de ses indicateurs, mais à sa capacité réelle à détecter les risques, à agir vite et à apprendre de ses erreurs. La qualité du dispositif dépendra moins de la complexité de ses outils que de la qualité des données, de la compétence des acteurs et de leur aptitude au jugement critique.

Références

- Agence Nationale d'Évaluation et d'Assurance Qualité de l'Enseignement Supérieur et de la Recherche Scientifique (ANEAQ) (2020). *Référentiel national d'évaluation et d'assurance qualité*.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2017). *Enterprise Risk Management; Integrating with Strategy and Performance*. COSO.
- Gallagher, M. (2012). *TEQSA and risk-based regulation*. Discussion Paper, Group of Eight (Go8), Australie.
- Higher Education Funding Council for England (HEFCE) (2012). *A risk-based approach to quality assurance: Consultation* (Publication 2012/11). Bristol: HEFCE.
- International Organization for Standardization (2018). *ISO 31000:2018 — Management du risque : lignes directrices*. Genève : ISO.
- Jackson, N. (2015). *Regulating higher education: Risk-based approaches to quality assurance*. Discussion Paper No. 79, Centre for Analysis of Risk and Regulation (CARR), London School of Economics and Political Science.

- King, R. (2015). *Risk-based quality assurance in higher education*. Discussion Paper, Centre for Analysis of Risk and Regulation (CARR), London School of Economics and Political Science.
- Loi-cadre n° 51-17 (2019). *Loi-cadre relative au système d'éducation, de formation et de recherche scientifique*. Royaume du Maroc, Bulletin officiel du 19 août 2019.
- National Center for Higher Education Management Systems (NCHEMS) (2017). *Risk-based approach to higher education accreditation: Concept paper*. Boulder : NCHEMS.
- Office for Students (2018). *Regulatory framework for higher education in England* et documents publiés sur l'approche fondée sur le risque et le suivi des établissements enregistrés. officeforstudents.org.uk
- Power, M. (2004). *The Risk Management of Everything: Rethinking the Politics of Uncertainty*. Londres : Demos.
- Power, M. (2007). *Organized Uncertainty: Designing a World of Risk Management*. Oxford: Oxford University Press.
- Quality Assurance Agency for Higher Education (QAA) (2018). *Data-driven risk-based quality regulation*. Gloucester: QAA.
- Strathern, M. (1997). « Improving ratings »: audit in the British University system. *European Review*, 5(3), 305-321.
- Tertiary Education Quality and Standards Agency (TEQSA) (2015). *A risk and standards-based approach to quality assurance in Australia's diverse higher education sector*. TEQSA.
- Tertiary Education Quality and Standards Agency (TEQSA) (2019). *Risk Assessment Framework* et documents associés sur l'approche fondée sur le risque. teqsa.gov.au
- U.S. Department of Education (2019). *Student Assistance General Provisions, Federal Pell Grant Program, and Federal Work-Study Programs* (Final Regulations, 34 CFR Parts 600 and 602). Washington, D.C.: Office of Postsecondary Education.
- U.S. Department of Education, Federal Student Aid (2023). *Financial responsibility composite score et Heightened Cash Monitoring* (Higher Education Act, §498). studentaid.gov; fsapartners.ed.gov

***CHAPITRE 3 : Digitalisation des processus douaniers et maîtrise des risques :
Enseignements pour la performance du contrôle dans le secteur public
marocain***

OURIACHI Nisrine Enseignante chercheure , KAMARY Nisrine, doctorante,
Entreprenariat, Marketing, Audit et Gouvernance -EMAG ,ENCGO-UMP- Oujda, Maroc

Les transformations rapides de l'environnement économique et géopolitique imposent aux États une adaptation continue afin de préserver leur compétitivité et leur efficacité dans un contexte de mondialisation et de fragmentation des chaînes de valeur. L'OCDE (2018) souligne dans son rapport *Trade Facilitation and the global Economy* que, cette fragmentation accroît la complexité des échanges transfrontaliers et renforce la nécessité de procédures commerciales efficaces. Dans ce contexte, les administrations publiques doivent moderniser leurs modes de fonctionnement afin de garantir l'efficacité des services, la transparence administrative et la résilience institutionnelle face à un environnement de plus en plus complexe.

Les administrations douanières occupent une position centrale dans la régulation des flux commerciaux internationaux et font face à une tension entre facilitation des échanges et sécurisation des frontières. La modernisation via les technologies de l'information et de la communication (TIC) apparaît ainsi essentielle pour concilier fluidité des procédures et lutte contre la fraude (Ishchuk et al., 2024). Cette évolution s'inscrit dans un cadre international porté par l'Accord sur la Facilitation des Échanges de l'OMC et dans la logique du New Public Management, où la digitalisation est perçue comme un levier de performance et de transparence (Yousfat et Menad, 2026). Toutefois, elle soulève également des enjeux de gouvernance et de gestion des risques, mis en évidence par la crise de la COVID-19, qui a révélé la nécessité de renforcer la résilience des chaînes logistiques et la continuité des services publics (Gutium, 2023 ; Yousfat et Menad, 2026).

Au Maroc, cette transformation numérique constitue une priorité nationale portée par la stratégie "Digital Morocco 2030", laquelle ambitionne d'améliorer le positionnement du Royaume dans les indicateurs de développement de l'e-gouvernement tout en restructurant en profondeur l'action publique (Bounou & Hattabi, 2025). Dans cette dynamique, l'Administration des Douanes et Impôts Indirects (ADII), acteur central de la régulation du commerce extérieur, s'est engagée dans un processus avancé de dématérialisation des procédures douanières. Depuis 2019, cette modernisation s'est traduite par la digitalisation des déclarations et l'automatisation progressive des mécanismes de contrôle (WCO, 2021).

Malgré un consensus croissant dans la littérature sur les effets positifs de la digitalisation sur la performance publique (Attaoui et Elmeziane, 2023 ; Ifiss, 2024), les connaissances demeurent limitées quant à ses effets combinés sur la performance du contrôle douanier et la maîtrise des risques dans les administrations publiques, particulièrement dans les pays en développement. Les études existantes, telles que celles de Karklina-Admine et al. (2024), Kim & Kim (2020) et Ishchuk et al. (2024), se concentrent principalement sur les pays développés

ou analysent séparément les dimensions de digitalisation, de performance et de gestion des risques, sans examiner suffisamment leurs interactions dans le contexte spécifique des administrations douanières. De plus, les enjeux liés à la gouvernance numérique, à la cyber-fraude ainsi qu'aux spécificités institutionnelles et organisationnelles du contexte marocain demeurent encore insuffisamment explorés. Dès lors, une tension persiste entre les gains d'efficacité liés à la digitalisation et les vulnérabilités qu'elle peut engendrer, ce qui conduit à la problématique suivante : comment la digitalisation des processus douaniers contribue-t-elle à améliorer la performance du contrôle et à renforcer la maîtrise des risques au sein de l'ADII ?

Pour répondre à cette interrogation, l'étude poursuit trois objectifs principaux : (i) analyser la contribution de la digitalisation à la gestion des risques douaniers ; (ii) identifier les risques persistants, notamment la cyber-fraude, malgré la transformation numérique ; et (iii) évaluer l'impact de cette transition sur la performance globale du contrôle douanier.

Sur le plan méthodologique, cette recherche adopte une approche mixte combinant analyse documentaire et entretiens semi-directifs auprès d'agents douaniers. Elle contribue théoriquement à la littérature sur la digitalisation des administrations publiques, le management des risques et la performance organisationnelle dans le contexte marocain, tout en apportant un éclairage empirique sur la transformation numérique du contrôle douanier. Sur le plan managérial, elle propose des recommandations visant à optimiser les processus de contrôle, renforcer la lutte contre la fraude et améliorer la satisfaction des opérateurs économiques. Enfin, l'article est structuré en trois parties : revue de littérature et cadre théorique, méthodologie, puis analyse et discussion des résultats.

1. Revue de littérature et cadre théorique

1.1. Cadre théorique de la performance publique et de la digitalisation

La compréhension du lien entre digitalisation, management du risque et performance du contrôle douanier s'inscrit d'abord dans des cadres théoriques issus des sciences de gestion et de l'administration publique. Parmi ces cadres, le courant du New Public Management (NPM), conceptualisé par Hood (1991), introduit dans les administrations publiques une logique de performance inspirée du secteur privé. Selon cet auteur, les organisations publiques doivent être évaluées à partir de résultats mesurables, de la productivité, de la réduction des coûts et de la responsabilisation des gestionnaires. Ainsi, la performance ne se limite plus au respect formel des procédures, mais renvoie à l'atteinte d'objectifs quantifiables et à l'optimisation des ressources. Dans le contexte douanier, cette approche implique l'analyse d'indicateurs tels que la réduction des délais de dédouanement, l'amélioration du taux de détection des fraudes,

l'optimisation des ressources humaines et budgétaires, ainsi que la satisfaction des opérateurs économiques. Cette orientation vers les résultats ouvre la voie à l'intégration d'outils modernes de gestion, notamment la digitalisation et le management du risque.

En complément de cette perspective, la théorie des capacités dynamiques développée par Teece, Pisano et Shuen (1997) apporte un éclairage déterminant. Elle soutient que la performance d'une organisation dépend de sa capacité à intégrer, construire et reconfigurer ses ressources internes et externes afin de s'adapter à un environnement changeant. Dans le contexte de la digitalisation des services publics, la technologie constitue une ressource stratégique, mais elle ne produit pas la performance en elle-même. Celle-ci résulte plutôt de la capacité organisationnelle à exploiter les outils numériques, à apprendre des données collectées et à ajuster en permanence les modèles de contrôle.

1.2. Clarification conceptuelle de la digitalisation et transformation numérique

La digitalisation est souvent confondue avec la numérisation ou la transformation digitale. Selon Verhoef et al. (2021), la numérisation correspond à la conversion d'informations analogiques en format numérique, sans transformation des processus sous-jacents. En revanche, la digitalisation implique une reconfiguration des activités et des modes de fonctionnement afin d'améliorer l'efficacité opérationnelle et de créer de la valeur (Allouche & Zerbib, 2020). Elle se distingue également de la transformation digitale, qui renvoie à une transformation stratégique globale de l'organisation (Varenne, 2020). Différentes perspectives enrichissent la compréhension de la digitalisation. Du point de vue business, elle permet de créer des revenus, d'améliorer les processus et d'intégrer l'information numérique au cœur des activités de l'organisation (Clerck, 2017). Dans une perspective socio-économique, elle constitue une transformation majeure de la société contemporaine, facilitant l'accessibilité, la transparence et de nouvelles formes de création de valeur (Hagberg et al., 2016). Sur le plan historique et économique, elle représente une synergie pervasive des innovations numériques dans l'ensemble de l'économie et de la société (Valenduc & Vendramin, 2017). Dans le marketing et la relation client, la digitalisation crée de nouvelles formes d'interaction entre les entreprises et leurs clients via des canaux numériques (Crittenden et al., 2019). D'un point de vue technologique et économique, elle réduit les distances, accroît la mobilité et permet l'exploitation des données pour répondre aux besoins individuels des consommateurs et des entreprises (Devereux & Vella, 2018). Enfin, elle englobe l'application croissante des TIC dans l'économie, incluant l'intelligence artificielle, l'Internet des objets et les concepts de la quatrième révolution industrielle (Morley et al., 2018). Dans le secteur public, la digitalisation

se traduit par l'e-gouvernement, qui utilise les technologies de l'information et de la communication (TIC) pour améliorer l'efficacité, la transparence et la prestation des services (Nations-Unies, 2018 ; OCDE, 2021).

1.3. Modernisation de l'administration publique et digitalisation des douanes

Au Maroc, la digitalisation des services publics s'inscrit dans un processus de réforme engagé depuis plusieurs décennies. Le programme e-Maroc 2010 a constitué un point de départ pour l'introduction des TIC dans l'administration. Cette dynamique a été poursuivie par le Plan Maroc numérique (2009–2013), puis par le Plan Maroc Digital 2020, avant d'être renforcée par la stratégie Digital Morocco 2030. La création de l'Agence de Développement du Digital en application de la loi n° 61-16 (Bulletin Officiel, 2017) et l'adoption de la loi 55-19 relative à la simplification des procédures administratives ont consolidé le cadre institutionnel de la transformation numérique. Les réformes engagées visent à simplifier les procédures, améliorer l'accès à l'information et généraliser la dématérialisation, en cohérence avec les orientations du Nouveau Modèle de Développement. Toutefois, malgré ces avancées, des défis persistent : en 2023, environ 92 % des citoyens et 87 % des entreprises se déclaraient non ou peu satisfaits des e-services existants (Chef du Gouvernement, 2020).

La douane, au cœur des échanges commerciaux internationaux, a un rôle stratégique au-delà de la simple collecte des taxes et droits : elle régule les flux commerciaux, assure la sécurité de la chaîne d'approvisionnement et facilite le commerce légal (OMD, 2006 ; Keen, 2003 ; Johnson, 2014 ; Bowman, 2006). Le dédouanement est défini comme l'accomplissement des formalités douanières permettant aux marchandises d'entrer, de sortir ou d'être placées sous un régime particulier (OMD, 2006). Ce processus est complexe, nécessitant une connaissance approfondie des réglementations, procédures et documents exigés (Johnson, 2014). Le contrôle douanier, selon l'OMD (2024), comprend l'ensemble des mesures visant à assurer l'observation des lois et règlements, tout en équilibrant la nécessité de contrôler les flux avec celle de faciliter le commerce légitime (OMD, 2024). Le contrôle douanier doit ainsi concilier deux objectifs parfois contradictoires : la sécurisation des recettes et la fluidité des échanges.

1.4. Management du risque douanier et apports des technologies numériques

Le management du risque douanier (Customs Risk Management – CRM), est défini par Drobot et al. (2017) comme une méthode logique et systématique d'identification, d'analyse et de traitement des risques associée à toute activité organisationnelle. Kim & Kim (2020) le considèrent comme un principe central du contrôle douanier moderne. Basir et al. (2019)

insistent sur son rôle dans l'allocation optimale de ressources limitées face à l'augmentation des volumes commerciaux. Par ailleurs, Satyadini et al. (2020) soulignent la nécessité d'un système dynamique intégrant l'intelligence artificielle afin d'anticiper les menaces dans un environnement global complexe.

L'adoption de l'IA, des mégadonnées, de la blockchain et du cloud computing est largement présentée comme un moteur de modernisation des douanes (Hakim et al., 2024 ; Chen, 2024 ; Wang, 2024 ; БеPECTOB et al., 2025). Ces technologies améliorent la détection des anomalies et des fraudes grâce à des analyses prédictives et à une sélectivité plus fine (Vijayakumar, 2025 ; Santos, 2024 ; Kim & Kim, 2020). Les systèmes automatisés de déclaration et de sélectivité réduisent les délais de dédouanement et les erreurs humaines (Ishchuk et al., 2024 ; Grafova & Bulgadaryan, 2023). Une enquête de l'OMD sur les douanes intelligentes, datant de juillet 2024, révèle que 62 % des membres ont participé, représentant 116 soumissions, et que 92 % d'entre eux ont mis en place une stratégie informatique, un élément clé de la digitalisation. Bien que les niveaux de maturité technologique les plus courants soient "opérationnel " (30 %) et "avancé" (27 %), le niveau "transformationnel" reste faible (7 %), indiquant un fort potentiel de croissance dans la transformation numérique des douanes (OMD, 2024). Toutefois, la littérature met également en évidence des divergences liées à la qualité des données, à la maturité technologique, aux coûts d'implantation et aux contraintes institutionnelles, particulièrement dans les pays en développement (Carpio, 2025 ; Hazapko, 2024 ; Pau & Alfimova, 2024 ; Zakhozhai et al., 2025). Des obstacles tels que les déficits d'infrastructure, les lacunes réglementaires et les pénuries de compétences sont fréquemment mentionnés (Hakim et al., 2024 ; Bilenets, 2024).

La digitalisation apparaît donc comme un levier central d'amélioration de la performance douanière, en renforçant la gestion des risques, la sélectivité des contrôles et l'efficacité administrative. Néanmoins, malgré le consensus sur ses effets positifs, il subsiste un manque d'études empiriques intégrant de manière systématique la digitalisation, la maîtrise des risques et la performance du contrôle en particulier dans les administrations douanières des pays en développement.

2. Méthodologie de recherche

Pour répondre à notre problématique, nous avons opté pour une étude de cas unique exploratoire, une approche particulièrement adaptée pour analyser un phénomène contemporain dans son contexte réel, lorsque les frontières entre le phénomène et son contexte ne sont pas clairement définies (Yin, 2018).

2.1. Le design de la recherche : Triangulation et validité

D'après Eisenhardt (1989), la rigueur des recherches de type théorie enracinée repose en partie sur la triangulation des méthodes de collecte de données. L'auteure souligne que les chercheurs mobilisent généralement plusieurs sources (entretiens, observations et données archivistiques) afin de renforcer la construction des concepts. Dans cette recherche, cette approche se traduit par la combinaison de sources secondaires, notamment le rapport d'activité de l'ADII (2024) et des articles scientifiques, ainsi que de données primaires issues d'entretiens semi-directifs réalisés sur le terrain.

2.2. Collecte des données

2.2.1. Analyse institutionnelle et documentaire

Selon Yin (2018), la documentation en étude de cas joue principalement un rôle de corroboration et d'enrichissement des données issues d'autres sources. Elle permet de vérifier des informations factuelles, de compléter des détails précis et de renforcer la fiabilité des résultats. En cas de contradictions avec d'autres sources, elle doit conduire à approfondir l'investigation plutôt qu'à être écartée. Afin de contextualiser les évolutions technologiques de l'ADII, nous avons procédé à une analyse de la documentation officielle. Bien que le Rapport d'activité 2024 de l'ADII constitue la pièce maîtresse de cette analyse, celle-ci a été complétée par des articles scientifiques et des publications institutionnelles traitant de la digitalisation douanière au Maroc.

2.2.2. Entretiens semi-directifs

La phase empirique de cette recherche repose sur la réalisation d'entretiens semi-directifs menés auprès d'acteurs au sein d'une administration douanière provinciale. Cette approche qualitative permet d'accéder aux perceptions, pratiques et expériences des agents.

- **Échantillonnage :** Un échantillonnage raisonné a été retenu afin de sélectionner quatre (4) inspecteurs des douanes, en raison de leur implication dans différents services complémentaires. Ce choix s'explique par la nature exploratoire de l'étude et la recherche d'une saturation théorique des données plutôt qu'une représentativité statistique.
- **Conditions de collecte :** Les entretiens ont été conduits en face à face, favorisant une interaction directe et une compréhension approfondie du contexte professionnel. Un guide d'entretien semi-structuré, organisé autour de trois axes principaux, a été mobilisé : (1) les pratiques liées à la digitalisation, (2) les contraintes et défis opérationnels, et (3) les perspectives d'amélioration et d'évolution des systèmes numériques.

- **Saturation des données :** La collecte des données a été interrompue après le quatrième entretien, conformément au principe de saturation théorique de Glaser et Strauss (1967, p. 61), selon lequel celle-ci est atteinte lorsqu'aucune information nouvelle ne permet de développer davantage les propriétés d'une catégorie. Dans cette recherche, la récurrence des discours autour du système BADR, des contraintes de connectivité et du besoin de renforcement des compétences numériques a confirmé cette saturation.

2.3. Processus d'analyse des données

Pour transformer les données brutes issues des entretiens en résultats analytiques, nous avons mobilisé l'analyse thématique, ou plus précisément l'analyse de contenu thématique (ACT). Cette méthode consiste à repérer, regrouper et analyser les thèmes récurrents présents dans un corpus de données verbales ou textuelles (Mucchielli, 1996, p. 259). L'analyse thématique vise ainsi à "procéder systématiquement au repérage, au regroupement et, subsidiairement, à l'examen discursif des thèmes abordés dans un corpus" (Paillé & Mucchielli, 2008, p. 162). Le processus d'analyse s'est déroulé en trois étapes :

- **Codage des données :** Chaque retranscription d'entretien a fait l'objet d'un découpage en unités de sens afin d'identifier des thèmes récurrents dans les discours des répondants. Des codes tels que "automatisation du système BADR", "lenteur du système", "formation continue" ou encore "intelligence artificielle et scanner" ont ainsi été relevés.
- **Catégorisation thématique :** Les codes identifiés ont ensuite été regroupés en catégories thématiques plus larges, structurées en fonction des objectifs de recherche, notamment : les apports de la digitalisation dans la gestion des risques, l'impact de la digitalisation sur la performance, ainsi que les risques identifiés dans le processus de contrôle douanier.
- **Synthèse et interprétation :** Enfin, les données ont été synthétisées afin de mettre en évidence les convergences observées, notamment autour de l'efficacité du système BADR, ainsi que les divergences ou points de vigilance, tels que la dépendance aux infrastructures numériques et les risques liés à la cybersécurité.

3. Résultats et discussion

3.1. Apports de la Digitalisation dans la gestion des risques

La digitalisation à l'ADII a instauré une gestion des risques proactive, s'appuyant sur des outils de ciblage intelligent. En 2024, l'analyse prédictive a permis de détecter 34 MDH de droits et taxes éludés (dont 20 MDH recouvrés) et de générer 5,39 MMDH de recettes additionnelles au titre de la valeur. Ce succès quantitatif repose sur une sélectivité dynamique. L'administration a mis en place 434 nouvelles règles de contrôle, permettant d'atteindre un taux

de sélectivité de 20,4 % à l'import et 8,9 % à l'export, optimisant ainsi le déploiement des inspecteurs sur le terrain. Ce dispositif est corroboré par les agents qui perçoivent le système comme un levier d'expertise. L'interviewé 1 précise : "Ce système est perçu comme un facilitateur qui améliore significativement la qualité du contrôle douanier [...] il permet d'identifier plus facilement les opérations à risque en analysant la première transaction effectuée par l'importateur, les implications fiscales de la marchandise et les antécédents de l'opérateur".

L'efficacité du système réside également dans sa capacité à automatiser les vérifications de cohérence, limitant les erreurs humaines. L'interviewé 4 souligne que le système BADR : "[...] signale les incohérences entre le montant total d'une facture et la somme des prix des articles. De même, il alerte les agents si une mainlevée est accordée à un opérateur qui n'a pas encore réglé ses droits et taxes". Enfin, l'interviewé 3 ajoute que cette gestion proactive s'appuie désormais sur des technologies de pointe pour sécuriser la chaîne logistique, notamment : "L'utilisation de l'intelligence artificielle pour analyser les images des scanners et repérer des anomalies, ainsi que le recours aux scellés électroniques et à la technologie RFID pour suivre les conteneurs en transit". Cette synergie entre outils décisionnels (SAAD) et outils opérationnels (BADR) permet à l'ADII de passer d'un contrôle de constatation à un contrôle d'anticipation, renforçant ainsi la crédibilité de l'action douanière.

3.2. Impact de la digitalisation sur la performance

L'impact de la dématérialisation sur la performance de l'ADII apparaît à la fois financier et opérationnel, comme en témoignent les indicateurs relatifs aux recettes douanières et à la lutte contre la fraude commerciale (Attaoui & El Meziane, 2023). Sur le plan financier, les recettes ont atteint 144,8 MMDH (+9,2 %). Sur le plan opérationnel, l'automatisation a réduit le délai de traitement des importations à 6 h 16, contre une réduction de 1 h 26 par rapport à l'année précédente. Les entretiens révèlent que cette performance est le fruit d'un changement de méthode. L'interviewé 2 affirme que la digitalisation "améliore la performance et réduit les délais et permet de contrôler moins et contrôler mieux". Cette notion de "contrôler mieux" est essentielle : avec 64 % des DUM obtenant la mainlevée en moins de 4 heures, l'efficacité est palpable. Il ajoute que l'accès rapide à l'historique des opérateurs permet de prendre des "décisions plus éclairées et plus rapidement".

Cette efficacité est quantifiée par les agents eux-mêmes, l'un d'eux estimant que "la digitalisation a transformé le travail des douaniers en facilitant la réalisation de leurs tâches quotidiennes dans une proportion de 80%" (Interviewé 4). L'aspect environnemental est également mis en avant comme un bénéfice direct de la dématérialisation : "L'opération se passe

désormais au niveau du système, sans papier" (Interviewé 2), confirmant l'alignement de l'ADII sur les objectifs de développement durable.

3.3. Risques identifiés dans le processus de contrôle douanier

La dématérialisation des procédures constitue un mode d'action publique visant à optimiser le fonctionnement interne de l'administration et à améliorer le service rendu aux usagers, dans une logique d'adaptation continue aux nouvelles contraintes (Aboutaoufik & Salam, 2021). Si la digitalisation a profondément modernisé l'ADII, l'analyse des entretiens révèle que cette transition n'est pas exempte de vulnérabilités. Les données recueillies permettent de catégoriser ces risques en trois axes majeurs.

- ❖ **Risques liés à la fraude commerciale** : Malgré un système capable de générer 5,39 MMDH de redressements en 2024, la fraude reste une menace hybride que la machine seule ne peut éradiquer. Les interviewés insistent sur le fait que la technologie est une aide, mais pas un substitut au flair douanier. L'interviewé 1 exprime cette réalité avec force : "Bien que la technologie puisse contribuer à la détection de la fraude en guidant les inspecteurs dans leur analyse, son utilisation seule n'est pas suffisante. Il est essentiel que l'inspecteur effectue ses propres vérifications et réfléchisse attentivement pour repérer la fraude. La technologie ne peut pas remplacer le jugement humain". Cette persistance de la fraude complexe est confirmée par le rebasculage de 4 % des déclarations du circuit orange vers le circuit rouge. L'interviewé 4 explique que le système aide à la décision en signalant des anomalies précises, comme "les incohérences entre le montant total d'une facture et la somme des prix des articles", mais que la validation finale reste humaine. Pour contrer ces risques, l'ADII mise sur une veille technologique constante, illustrée par le Digital Douane Lab (DDLab) qui, selon l'interviewé 3, "développe des outils d'innovation pour la prévention des fraudes", rejoignant ainsi les perspectives d'intégration de l'IA étudiées par Basri et al. (2024).
- ❖ **Risques liés aux partenaires institutionnels** : Le contrôle douanier s'inscrit dans un écosystème complexe incluant la NARSA, l'ONSSA, le ministère de la Santé ainsi que d'autres parties prenantes. La digitalisation de l'ADII ne peut être pleinement efficace que si ses partenaires suivent le même rythme. L'interviewé 4 note que la digitalisation simplifie le recoupement des informations, mais que la dépendance aux données externes reste un point de vigilance : "La digitalisation fiabilise l'information et facilite le recoupement avec d'autres administrations, afin de vérifier l'exactitude des données déclarées". Cependant, les retards de réponse des partenaires institutionnels peuvent encore paralyser la mainlevée,

créant des goulots d'étranglement que seule une généralisation de la digitalisation partagée pourrait résorber.

- ❖ **Risques technologiques :** Le risque le plus cité par les agents est celui de la "paralysie numérique". La performance opérationnelle, mesurée par un délai moyen de 6h16 à l'import, est tributaire d'une infrastructure sans faille. L'interviewé 4 alerte sur cette vulnérabilité : "Les problèmes de connexion internet peuvent entraîner des retards significatifs dans le traitement des dossiers. Il est impératif de mettre en place un "plan B" afin de garantir la continuité des opérations en cas de défaillance du système". L'interviewé 1 abonde dans ce sens, soulignant que "l'un des principaux inconvénients de la dématérialisation est que, en cas de dysfonctionnement de l'intranet, l'inspecteur se retrouve incapable de travailler". Au-delà des pannes, la menace de cyberattaques (comme celles recensées en 2025 sur d'autres plateformes, notamment Oracle et PortNet) est prise très au sérieux. L'interviewé 4 recommande ainsi de "renforcer la protection du système d'information contre les cyberattaques et de former les agents aux bonnes pratiques en matière de cybersécurité". Enfin, l'obsolescence des compétences est identifiée comme un risque managérial majeur. L'interviewé 3 résume ce besoin d'accompagnement : Un inconvénient de la digitalisation est le besoin constant de formation et d'accompagnement. Avec l'évolution rapide des technologies, il est indispensable d'organiser d'autres sessions pour maintenir les compétences à jour".

D'après ces résultats, la digitalisation au sein de l'ADII a considérablement renforcé la performance du contrôle douanier, en rendant les opérations plus efficaces, transparentes et fluides, tout en simplifiant le travail des agents. Elle favorise un ciblage précis des risques et une meilleure traçabilité des échanges. Néanmoins, la persistance de fraudes, les dépendances institutionnelles et les vulnérabilités technologiques soulignent la nécessité de combiner outils numériques, contrôle humain et coordination inter-institutions pour sécuriser pleinement le système.

Théoriquement, ces observations confirment les principes du New Public Management, qui valorisent des indicateurs de performance mesurables et l'optimisation des ressources, ainsi que la théorie des capacités dynamiques, montrant que la performance dépend de la capacité à exploiter les technologies et à s'adapter à un environnement en évolution.

Sur le plan managérial, l'expérience de l'ADII démontre l'importance d'une approche intégrée, alliant digitalisation, formation des agents, optimisation des processus et coordination

inter-institutions, pour maximiser l'efficacité, renforcer la transparence et sécuriser la chaîne logistique.

4. Conclusion

Cette recherche avait pour objectif principal d'analyser l'effet de la digitalisation sur l'amélioration de la performance et la gestion des risques des processus douaniers, en prenant le cas de l'ADII, l'administration douanière marocaine. Les résultats ont été collectés à travers la documentation, ainsi que des entretiens semi-directifs réalisés auprès des agents douaniers afin de recueillir leurs perceptions réelles, au-delà des rapports officiels qui peuvent présenter uniquement des résultats positifs, afin de préserver la sincérité de l'analyse.

Les résultats convergent vers une réalité : la digitalisation a un effet positif sur le contrôle douanier. Elle permet d'améliorer la performance et de gérer les risques de manière efficace. La modernisation progressive de l'administration, chaque année, renforce l'efficacité et la détection des fraudes, démontrant que l'ADII est agile, flexible et à jour avec les tendances technologiques, facilitant ainsi le commerce et le mouvement transfrontalier. Malgré ces apports, certains risques persistent. La fraude, notamment la sous-déclaration ou les manipulations des codes SH (Système Harmonisé) ou des quantités, reste préoccupante et souvent en hausse. Les risques technologiques et de cybersécurité nécessitent une formation continue et le renforcement des dispositifs de protection pour sécuriser les informations des opérateurs économiques.

Comme toute recherche, cette étude présente des limites, notamment méthodologiques. Pour obtenir des résultats plus représentatifs et influents, il serait pertinent de réaliser des entretiens semi-directifs dans les différentes directions régionales et provinciales afin de collecter des perceptions variées. Des disparités technologiques peuvent exister entre les régions, par exemple entre Casablanca-Settat et l'Oriental. Des études comparatives avec d'autres administrations, arabes ou européennes, pourraient également permettre d'analyser les convergences et divergences dans les pratiques et les effets de la digitalisation.

Face aux risques identifiés, il est recommandé de renforcer la digitalisation de l'ADII en intégrant des outils d'intelligence artificielle pour l'analyse des risques et le ciblage des déclarations suspectes, ainsi que des technologies d'inspection non intrusive combinant scanners et IA. Il convient également de moderniser le système BADR via une migration vers une architecture cloud plus stable, d'explorer l'usage de la blockchain pour sécuriser et tracer les documents douaniers, et d'exploiter l'Internet des objets (IoT) pour assurer un suivi en temps

réel des marchandises. Enfin, le renforcement du dispositif de cybersécurité apparaît essentiel afin de prévenir les intrusions et les cyberattaques, garantissant ainsi une performance durable et une meilleure sécurisation de la chaîne logistique.

5. Références

- ✓ Aboutaoufik, A., & Salam, G. (2021). Retour sur l'expérience de l'administration numérique au Maroc : cas des douanes et impôts indirects et de PortNet. HALSHS.
- ✓ Allouche, J., & Zerbib, R. (2020). La transformation digitale : Enjeux et perspectives. *La Revue des Sciences de Gestion*, 301-302(1-2), 75–76.
- ✓ Association of Certified Fraud Examiners (ACFE). (2012). Report to the nation on occupational fraud and abuse.
- ✓ Attaoui, H., & El Meziane, A. (2023). Le digital et la performance de l'action de la douane au Maroc. *African Scientific Journal*, 3(19), 863–889.
- ✓ Basir, A., Satyadini, A. E., & Barata, A. (2019). Modern customs risk management framework: Improvement towards institutional reform. *International Journal of Innovative Science and Research Technology*, 4, 60–69.
- ✓ Basri, N., Garouaz, S., Charfi, M., & Moussamir, A. (2024). L'intégration de l'IA dans l'administration des douanes marocaines : approche prospective stratégique. *African Scientific Journal*, 3(25), 632.
- ✓ Bilenets, D. (2024). Protection of digital infrastructure in customs-administrative services: Challenges and modern approaches to cybersecurity. *Analytical and Comparative Jurisprudence*, 47, 301–306.
- ✓ Bounou, S. E., & Hattabi, J. (2025). La transition numérique au Maroc : analyse des enjeux et des dynamiques d'une action publique. *Revue Marocaine des Politiques Publiques*, 1(28), 19–31.
- ✓ Bowman, G. W. (2006). Thinking outside the border: Homeland security and the forward deployment of the US border. *Houston Law Review*, 44(2), 189–251.
- ✓ Carpio, T. A. G. (2025). Aduanas inteligentes y sostenibles: Innovación tecnológica y su relación con el desarrollo humano. *Revista Internacional De Desarrollo Humano Y Sostenibilidad*, 2(2), 11–35. <https://doi.org/10.51660/ridhs22324>
- ✓ Chen, Z. (2024). AI-powered customs clearance: Optimizing trade compliance and border management. *Journal of AI-Driven Trade Facilitation Engineering and Single Window Systems*, 1(1), 79–98. <https://doi.org/10.6914/sw.010105>
- ✓ Clerck, J. (2017). Digitalization, digital transformation: The differences. *i-SCOOP*.

- ✓ Crittenden, W. F., Biel, I. K., & Lovely, W. A. (2019). Embracing digitalization: Student learning and new technologies. *Journal of Marketing Education*, 41(1), 5–14.
- ✓ Devereux, M., & Vella, J. (2018). Debate: Implications of digitalization for international corporate tax reform. *Intertax*, 46(6), 550–559.
- ✓ Drobot, V. E., Klevleeva, A. R., Afonin, P. N., & Gamidullaev, S. N. (2017). Risks management in customs control. *Economy of Region*, 13, 551–558.
- ✓ Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review*, 14(4), 532–550.
- ✓ Grafova, T., & Bulgadyan, A. (2023). Customs control using artificial intelligence technologies. *Jurnal BPPK: Badan Pendidikan Dan Pelatihan Keuangan*, 16(2), 121–130.
- ✓ Gutium, M. P. (2023). Development of the digitalization of the customs service in the Republic of Moldova. *Information and Innovations*, 18(2), 48–55.
- ✓ Hagberg, J., Sundström, M., & Egels-Zandén, N. (2016). The digitalization of retailing: An exploratory framework. *International Journal of Retail & Distribution Management*, 44(7), 694–712.
- ✓ Hakim, S., Sukmana, S. D., Dermawan, H., Arevin, A. T., & Muchayatin, M. (2024). Integrating AI and blockchain technologies for enhanced risk management and operational efficiency in Indonesian airport customs: Challenges and opportunities. *Journal of Social Science*, 1(6), 283–295. <https://doi.org/10.59613/tdxck922>
- ✓ Ishchuk, M., Ishchuk, O., Khrypko, S., Shnitser, M., Vasylchuk, T., Syhyda, H., & Hotsalyuk, A. (2024). Sustainable digital evolution: Transforming the Ukrainian customs service. *European Journal of Sustainable Development*, 13(1), 217.
- ✓ Johnson, T. E., & Bade, D. L. (2014). *Export/import procedures and documentation* (4th ed.). AMACOM.
- ✓ Kim, S.-B., & Kim, D. (2020). ICT implementation and its effect on public organizations: The case of digital customs and risk management in Korea. *Sustainability*, 12(8), 3421.
- ✓ Michael, K. (2003). *Changing customs: Challenges and strategies for reform of customs administration*. IMF.
- ✓ Morley, J., Widdicks, K., & Hazas, M. (2018). Digitalisation, energy and data demand: The impact of internet traffic on overall and peak electricity consumption. *Energy Research & Social Science*, 38, 128–137.
- ✓ OCDE. (2021). *Perspectives de l'économie numérique de l'OCDE 2020 (Version abrégée)*. Éditions OCDE. <https://doi.org/10.1787/3b257711-fr>

- ✓ OMD. (2006). Convention internationale sur la simplification et l'harmonisation des régimes douaniers (Convention de Kyoto révisée), annexe générale, chapitre 6 : Contrôle douanier. OMD.
- ✓ OMD. (2024). Glossaire des termes douaniers internationaux.
- ✓ OMD. (2024). Projet sur les douanes intelligentes : Résultats de l'enquête de l'OMD sur les douanes intelligentes.
- ✓ Royaume du Maroc, Le Chef du Gouvernement. (2020). Note d'orientations générales pour le développement du digital au Maroc à horizon 2025.
- ✓ Santos, D. (2024). Enhancing international trade security: Real-time risk assessment in Brazilian customs with blockchain technology. *International Journal of Business and Management*, 19(6), 49–61. <https://doi.org/10.5539/ijbm.v19n6p49>
- ✓ Satyadini, A. E., Basir, A., & Barata, A. (2020). A cutting-edge approach to risk management framework: Upswing customs administration. *Journal of Management Research*, 12, 57–73.
- ✓ United Nations, Department of Economic and Social Affairs. (2018). E-government survey 2018: Gearing e-government to support transformation towards sustainable and resilient societies (pp. 1–10). United Nations.
- ✓ Valenduc, G., & Vendramin, P. (2017). Digitalisation, between disruption and evolution. *Transfer: European Review of Labour Research*, 23(2), 121–134.
- ✓ Varenne, P. (2020). La transformation digitale des entreprises : Effectuation et Business Model Digital Dynamique (BMD2) (Thèse de doctorat, Université de Lyon, France).
- ✓ Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*, 122, 889–901.
- ✓ Vijayakumar, S. (2025). Technology-centric and data-driven customs risk management for supply chain security. *World Customs Journal*, 19(1), 38–63.
- ✓ Wang, A. (2024). Leveraging machine learning for predictive analytics in trade facilitation engineering. *Journal of AI-Driven Trade Facilitation Engineering and Single Window Systems*, 1(1), 62–78. <https://doi.org/10.6914/sw.010104>
- ✓ Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). Sage.
- ✓ Yousfate, A. (2026). Big data management and digital transformation in government institutions – local and international models. *Journal of Management and Organizations Strategy*, 8(1), 19–31.

- ✓ Zakhozhai, K., Борошенко, Т. М., & Kolomiets, H. (2025). Post-clearance customs audit within the state's economic security risk management framework amid global shocks. *Економічний простір*, 202, 115–124. <https://doi.org/10.30838/EP.202.115-124>
- ✓ Берестов, І. В., Пестременко-Скрипка, О. С., & Колісник, А. В. (2025). Implementation of the latest technologies for carrying out customs control during transportation of cargo by rail transport. *Zbirnyk naukovykh prats UkrDUZT*, Issue 211, 269–277.
- ✓ Назарко, А. А. (2024). Customs competencies in Ukraine: Implementing innovations to enhance efficiency. *Аналітично-порівняльне правознавство*, 5, 587–592.

CHAPITRE 4: *Financial risk auditing and industrial performance: An integrative conceptual framework*

Marouane EL ALITI, (*Doctoral student*) , **Omar TAOUAB**, (*Professor-Researcher*)
National School of Commerce and Management- Ibn Tofail University, Kénitra, Morocco
marouane.elaliti@uit.ac.ma

Industrial firms today face unprecedented volatility, regulatory pressure, and supply chain disruptions. In this context, the pursuit of performance is inseparable from organizational resilience (Lengnick-Hall et al., 2011). Industrial organizations, particularly within the Moroccan context, face the dual challenge of adapting to uncertainty while optimizing their production systems. This reality raises questions about the role of traditional support functions, particularly financial risk auditing. Historically confined to a retrospective, accounting-based control function, financial risk auditing may hold critical intelligence on organizational vulnerabilities. However, its impact on operational performance often remains indirect, if not overlooked, due to a persistent disconnect between financial control logics and operational value-creation imperatives.

This tension raises a central strategic question: How can financial risk auditing transcend its traditional accounting control function to become a forward-looking diagnostic tool for operational vulnerability, thereby providing real-time input for strategic decisions that simultaneously enhance resilience and optimize the sustainable performance of industrial operations? This question calls for a reconceptualization of financial risk auditing, moving beyond its traditional role as a compliance or risk-mitigation device toward recognition as a strategic lever for performance optimization and organizational resilience. This study draws on three complementary theoretical perspectives: agency theory (Jensen & Meckling, 1976), the resource-based view (Barney, 1991), and dynamic capabilities (Teece et al., 1997).

To address this problem, this research establishes three primary objectives. First, to analyze the theoretical and practical mechanisms through which information and recommendations from financial risk audits can influence the operational and strategic decisions of industrial managers. Second, to assess the potential impact of these mechanisms on key industrial performance indicators, such as productivity, profitability, and cost control. Ultimately, with a prescriptive aim, this proposal seeks to provide an integrative framework and operational recommendations that enable organizations to systematically enhance their strategic leveraging role.

The contributions of this research are both theoretical and practical. From an academic standpoint, it aims to enrich an emerging interdisciplinary literature at the intersection of enterprise risk management, understood as a strategic capability (Florio & Leoni, 2017), modern internal auditing, and performance management control by adopting an integrated analytical approach to domains that are often examined in isolation. From a managerial perspective, this article aims to provide decision-makers, such as executives, internal auditors, management controllers, and operational managers, with actionable insights to better align

auditing mechanisms with industrial performance objectives, thereby fostering more integrated and resilient governance.

This article is structured as follows. First, we establish the theoretical foundations through a critical review of the literature focusing on the strategic evolution of financial risk auditing and its relationship with industrial performance. Second, we present the research methodology, which adopts a conceptual approach based on a structured, critical, and integrative review of the academic literature. This approach aims to deconstruct existing paradigms and to develop a novel analytical study that repositions financial risk auditing as a strategic lever for industrial performance and organizational resilience. Third, we develop and discuss the main analytical insights and conceptual propositions derived from the literature, highlighting the key mechanisms through which financial risk auditing can influence operational resilience and performance optimization. Finally, we conclude by synthesizing the article's main contributions, discussing their theoretical and managerial implications, acknowledging the study's limitations, and outlining directions for future research.

1. Literature review and theoretical framework

The primary source of uncertainty for industrial enterprises stems from financial risks, which, among other things, directly affect operational efficiency, strategic decision-making, and overall organizational performance. To develop a deeper understanding of how financial risk audits can be transformed from a traditional control function into a strategic tool for industrial performance and resilience, we must comprehend the taxonomy and nature of financial risks.

1.1. Taxonomy of financial risks in industrial firms

The materiality of its operations fundamentally shapes an industrial firm's financial risk profile. Unlike service-based entities, industrial organizations are exposed to distinct financial vulnerabilities arising from heavy capital investment, complex global supply chains, elongated production cycles, and the physical transformation of inputs into finished goods (Brealey et al., 2020). This embeddedness of financial risk within operational processes necessitates a taxonomy that moves beyond generic categorizations. The following analysis classifies these risks into four core types to delineate the specific terrain that financial risk navigates in this sector.

Industrial activities are inherently capital-intensive and characterized by a protracted cash conversion cycle. Significant funds are immobilized in raw material inventories, work-in-progress, and finished goods, while trade credit extended to customers further delays cash inflows (Brigham & Ehrhardt, 2020). This structural mismatch between cash outflows and inflows creates a persistent liquidity risk. A disruption in this cycle, whether from production

delays, inventory obsolescence, or extended customer payment terms, can swiftly jeopardize solvency, making the management of working capital a critical financial imperative and a focal point for audit scrutiny.

Industrial firms often exhibit concentrated dependency on a limited number of key suppliers for critical components and on major clients for a substantial portion of revenue. This concentration amplifies credit risk, the risk of financial loss due to a counterparty's failure to meet its obligations (Saunders & Cornett, 2018). The default of a strategic supplier can halt production lines, while the insolvency of a major client can cripple cash flow. Therefore, auditing must assess not only the financial health of these counterparties but also the resilience of the procurement and sales portfolios.

Globalized industrial operations are acutely exposed to volatility in input costs and exchange rates. Fluctuations in the prices of key commodities (e.g., metals, energy, agricultural products) directly impact production costs and profit margins. Concurrently, revenues and costs denominated in foreign currencies introduce translation and transaction exposures (Hull, 2018). For industries with thin margins, such volatility can erase profitability. Auditing, therefore, must evaluate the adequacy of hedging strategies and the sensitivity of financial projections to these external market variables.

This category encompasses financial risks emanating directly from operational inefficiencies and capital allocation decisions. It includes cost overrun risk, in which actual production costs exceed standards due to waste, inefficiency, or supplier price hikes, and investment (or capital expenditure) risk, associated with the misallocation of capital into projects that fail to yield expected returns or become technologically obsolete (Eulerich & Eulerich, 2020). These risks lie at the nexus of operational management and financial performance, representing a critical interface where audit insights can translate into tangible value preservation.

This taxonomy illustrates that financial risks in the industrial sector are not abstract accounting concepts but are deeply interwoven with tangible assets, physical processes, and strategic decisions. Their effective management, and by extension, their auditing, demands an understanding that bridges the finance and operations divide. Having delineated this risk landscape, the analysis now turns to the function tasked with its assessment: the evolution and current paradigm of financial risk auditing.

1.2.The paradigm of financial risk auditing: From control function to strategic assurance

The practice and perceived purpose of financial risk auditing have undergone a profound conceptual shift over recent decades. This evolution mirrors the broader recognition of risk management as a strategic capability rather than a mere defensive control. To appreciate how

auditing can function as a lever for industrial performance, it is essential to trace its trajectory from its origins in financial verification to its contemporary aspiration to provide strategic assurance and foresight.

Traditionally, the role of internal auditing has been predominantly one of financial control and regulatory compliance. It has been retrospective, focusing on verifying the accuracy of accounting records, detecting fraud or errors, and determining compliance with relevant laws and internal policies (Mautz & Sharaf, 1961). In this paradigm, the auditor acted as an independent verifier, often perceived by operational management as an external inspector or a necessary constraint. In this paradigm, the auditor acted as an independent verifier, often perceived by operational management as an external inspector. The scope was largely confined to financial transactions, with limited engagement in business process improvement or strategic advisory.

A fundamental shift began with the widespread adoption of risk-based auditing. This approach, now codified in professional standards such as those of the Institute of Internal Auditors (IIA, 2017), reoriented the audit process around the organization's most significant risks. Instead of cyclical reviews of all areas, audit plans are derived from a dynamic risk assessment, prioritizing resources toward the processes, units, or topics presenting the highest potential impact (COSO, 2004). This change marks a significant shift in how auditing is conducted; rather than reviewing what has occurred, auditing now evaluates what could go wrong, aligning the audit function more closely with management's risk mitigation strategies and organizational priorities.

Building on this risk-centric foundation, the contemporary paradigm positions internal auditing as a provider of strategic assurance and consulting services. The IIA's definition of internal audit as an activity that "helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes" explicitly includes consulting and advisory roles (IIA, 2017). As a result, the auditor's role transforms from being simply a controller who provides hindsight coverage to providing anticipatory advice by assessing potential risk exposures, evaluating the effectiveness of an organization's Enterprise Risk Management (ERM) frameworks, and identifying opportunities to strengthen organizational resilience and value creation (Florio & Leoni, 2017). The function's value proposition is thus reconceptualized from protecting existing value to enabling future performance (Sarens & De Beelde, 2006).

This evolution aligns with agency theory (Jensen & Meckling, 1976), which posits that auditing reduces information asymmetry between managers and shareholders, thereby improving decision-making quality and reducing opportunistic behavior.

Despite the evolution of financial risk auditing toward strategic assurance, the literature indicates that its direct influence on operational aspects of industrial performance, such as production efficiency, cost control, and quality, remains underexplored. The majority of available literature focuses on governance, compliance, and financial reporting, resulting in a limited description of the connection between insights gained from financial risks and the development of actionable decisions for operational management through the use of financial risk assurance in building/operating profitable companies. This understanding is necessary to fully comprehend the impact that financial risk auditing can have on industrial performance.

1.3. Financial risk auditing and industrial performance

The relationship between financial risk auditing and industrial performance has received increasing attention in the academic literature, yet its operational mechanisms remain insufficiently theorized. While internal auditing has evolved from control to strategic assurance, its direct contribution to operational performance drivers, such as productivity, cost efficiency, and quality, is often addressed indirectly. Existing studies emphasize governance and financial reporting, whereas the pathways from audit insights to shop-floor improvements are less articulated (Beasley et al., 2005; Florio & Leoni, 2017).

Financial risk auditing enhances the example of industrial performance by providing information and diagnostics that support decision-making by systematically identifying, assessing, and communicating financial risk exposures. This ability to generate unique knowledge about operational vulnerabilities is in line with the Resource-Based View (Barney, 1991), which considers auditing as a strategic organizational resource that creates value. As a result, the quality and relevance of the information that is available to management for decision-making are improved. In capital-intensive, complex production processes and through interdependent supply chains, such risk intelligence at the industrial level can facilitate more informed investment planning, the management of working capital, the development of cost structures, and the allocation of resources (COSO, 2017). In this sense, financial risk auditing serves as a mechanism that reduces uncertainty and improves the rationality of decision-making at both strategic and operational levels.

The literature further suggests that financial risk auditing plays a complementary role in strengthening organizational resilience, a dimension increasingly recognized as a critical component of sustainable industrial performance. By anticipating potential financial

disruptions embedded in operational processes, such as liquidity constraints, supplier dependency, or exposure to volatile input prices, auditing enables proactive risk mitigation and adaptive responses (Lengnick-Hall et al., 2011). Furthermore, this forward-looking perspective is also consistent with viewing risk management as an organizational capability that assists a firm's ability to respond effectively to shocks, continue operations, and maintain performance in an uncertain environment (Florio & Leoni, 2017).

Although there are some theoretical insights into how financial risk auditing can be used to improve industrial performance, such as productivity, cost efficiency, quality, and reliability of delivery, there is still a significant gap in the existing literature regarding the development of the specific ways in which financial risk auditing affects different aspects of industrial performance. Most contributions stop short of explicitly linking audit outputs (e.g., risk assessments, control evaluations, audit recommendations) to operational actions and performance improvements within industrial processes. As a result, the relationship between financial risk auditing and performance is assumed rather than systematically conceptualized. Overall, the existing literature supports the notion that financial risk auditing holds significant potential to influence industrial performance, particularly when embedded within a strategic, risk-based orientation. However, a coherent theoretical framework integrating financial risk auditing with the multiple dimensions of industrial performance remains to be developed (Power, 2007).

2. Research methodology

This study adopts a conceptual research design grounded in a structured, critical, and integrative review of the academic literature, an approach commonly used to develop new theoretical frameworks in emerging or fragmented research areas (Jaakkola, 2020). Rather than relying on empirical data, the article seeks to develop a coherent theoretical understanding of the relationship between financial risk auditing and industrial performance. The objective is to synthesize dispersed contributions from the fields of internal auditing, risk management, and operations management to construct an integrative conceptual framework.

The research follows a deductive and integrative reasoning process. First, the literature on financial risks in industrial firms is examined to identify the main categories of risks and their operational implications. Second, the evolution of financial risk auditing is analyzed, highlighting the transition from a traditional control-oriented function to a strategic assurance role. Third, the literature on industrial performance is mobilized to clarify its multidimensional nature and its key operational drivers. These three streams of literature are then conceptually connected to identify theoretical complementarities and persistent gaps.

The literature review is conducted through a structured selection of academic sources, including articles from specialized journals indexed in databases such as Scopus and Web of Science, institutional frameworks, and reference works on auditing, risk management, and operational performance. The research primarily targeted peer-reviewed articles published between 2000 and 2025, a period covering the major evolution of auditing toward a strategic assurance function. Theoretical and empirical contributions directly related to the three identified streams were retained, while non-academic sources or those without an explicit link to the relationship between audit and performance were excluded. Priority is given to theoretical contributions and to widely recognized empirical studies that shed light on the relationships among auditing, risk, and performance. The analysis aims to identify recurring concepts, theoretical mechanisms, and points of convergence or divergence in the literature.

Based on this integrative analytical process, the article develops a conceptual research that positions internal auditing as a potential driver of industrial performance. However, the proposed model is not intended to provide empirical validation but rather to clarify the theoretical mechanisms linking outputs from financial auditing, such as risk assessments, control evaluations, and audit suggestions, to improvements in operational dimensions.

3. An integrative framework linking financial risk auditing and industrial performance

Building on the theoretical foundations established in the literature review, an integrative framework to address the identified gap: the lack of a unified model outlining how financial risk auditing leads to improved industrial performance. The research synthesizes knowledge from financial risk management, strategic auditing, and industrial performance research to develop a structured conceptual framework of the audit-performance nexus. Rather than offering empirical validation, this study provides a lens for understanding the mechanisms at play and for guiding future empirical investigation.

The proposed framework rests on three interconnected components: inputs, processes, and outcomes. The inputs consist of the tangible and intangible outputs of the financial risk audit function, consistent with the governance and assurance responsibilities placed on internal audit within modern frameworks (IIA, 2017). These include formal deliverables such as risk assessment matrices, control deficiency reports, and audit recommendations, as well as informal outputs such as enhanced risk awareness and improved communication between auditors and operational managers. As noted in previous research on the effectiveness of the internal audit function (Sarens & De Beelde, 2006), however, audit outputs do not automatically produce performance improvements; rather, they rely on processes within organizations to facilitate interpretation, decision-making, and action.

The audit results can be translated into performance outcomes through three key organizational mechanisms. The first is the informational mechanism, through which audit findings enhance the quality of managerial decision-making. By providing reliable, timely, and risk-focused information, auditing strengthens governance and control systems, in line with the broader perspective of management control frameworks (Simons, 1995). With better intelligence about the financial risks they face, such as liquidity problems, cost overruns, or currency-related risks, managers can optimize production scheduling, inventory levels, and investment timing. This directly impacts organizational operational performance. The second is the corrective mechanism, whereby audit recommendations trigger targeted remediation actions. When control deficiencies are addressed or process inefficiencies are corrected, organizations reduce waste and prevent financial losses. This illustrates the changing nature of the internal audit function, from one focused on compliance to a valuable contributor to governance structures (Gramling et al., 2004). The third mechanism emphasizes both cultural and pedagogical learning processes. Repeated audit interactions contribute to the development of a risk-aware organizational culture and foster collective learning. This is consistent with organizational learning theory (Argyris & Schön, 1978) and dynamic capabilities (Teece et al., 1997), which emphasize the firm's ability to adapt, reconfigure resources, and respond proactively to emerging risks. Through this cultural mechanism, financial risk auditing strengthens the resilience of sustainability and long-term performance.

The conceptual relationships identified in the literature are synthesized in the following integrative framework, which illustrates the mechanisms by which financial risk auditing contributes to the improvement of industrial performance.

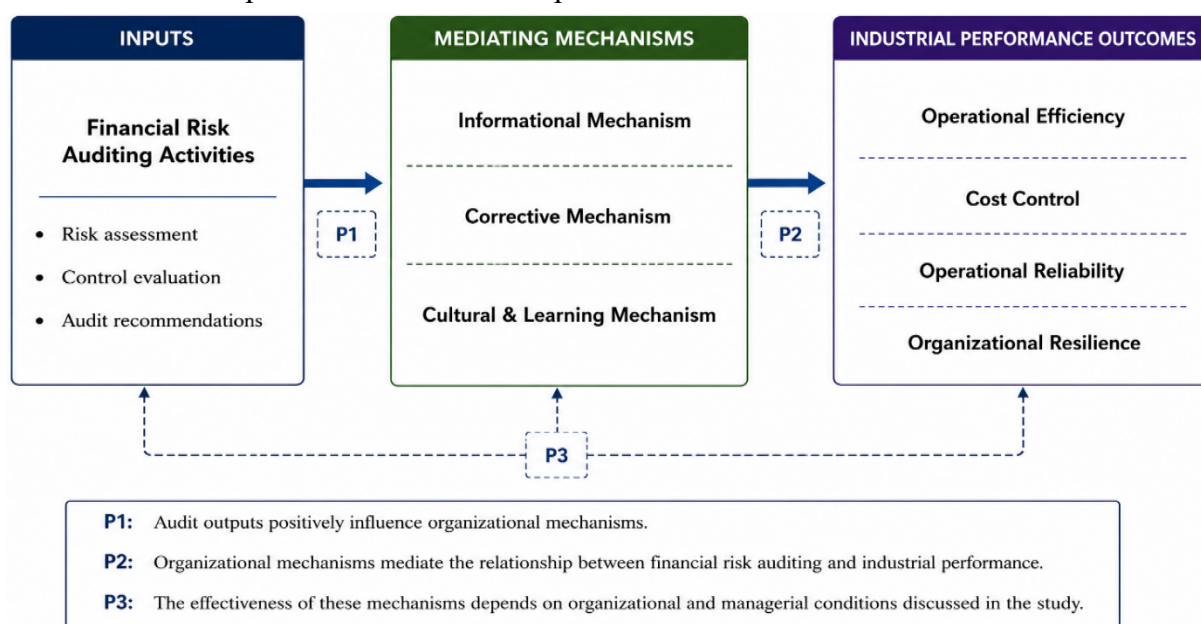


Figure 1: Conceptual framework linking financial risk auditing to industrial performance

As illustrated in Figure 1, the proposed framework conceptualizes financial risk auditing as a strategic organizational capability influencing industrial performance through informational, corrective, and cultural mechanisms. The model also highlights the mediating role of organizational processes in transforming audit activities into operational results and resilience capabilities.

The framework yields three formal theoretical propositions:

- H1: The quality and relevance of financial risk audit outputs positively influence the effectiveness of organizational translation mechanisms.
- H2: These organizational mechanisms mediate the relationship between audit outputs and improvements in industrial performance dimensions.
- H3: The strength of these mechanisms is contingent upon contextual factors such as management commitment, cross-functional integration, and risk culture maturity.

The outcomes of these mechanisms materialize across the multidimensional spectrum of industrial performance. In line with established operations management literature (Skinner, 1969; Slack, 1991), industrial performance encompasses productivity, cost efficiency, product quality, and operational flexibility. Financial outcomes such as improved profitability and capital allocation efficiency are closely intertwined with these operational dimensions. Importantly, these performance dimensions are mutually reinforcing: operational stability supports financial performance, while financial discipline enhances operational robustness.

The analysis yields three theoretical propositions. First, the quality and relevance of audit outputs related to financial risk will positively impact the effectiveness of organizational translation mechanisms (Liu et al., 2025). Second, these organizational mechanisms mediate the relationship between audit outputs and improvements in industrial performance dimensions. Third, the strength of this mediation depends upon contextual factors such as managerial commitment, integration between audit and operational functions, and the maturity of the organization's risk culture.

In summary, this integrative framework positions financial risk auditing not only as a compliance or control function but also as a strategic lever for optimizing industrial performance. By specifying the informational, corrective, and cultural mechanisms that link audit outputs to operational improvements, this framework fills a persistent theoretical gap. It provides a coherent basis for future empirical research and managerial applications.

4. Discussion and implications

The integrative framework provides a coherent response to the primary theoretical gap in this industrial performance literature: the lack of a clear model that illustrates how financial risk

auditing impacts the specific dimensions of industrial performance. By specifying three mediating mediators for each function, namely informational, corrective, and cultural, this model goes beyond simply assuming that there is a direct relationship between auditing and performance and instead defines auditing as a collection of processes used within an organization to impact operational outcomes indirectly. In other words, this present research provides a structured approach to understanding how audit output transforms into improvements in efficiency, reliability, and adaptability.

From a theoretical standpoint, the framework contributes to the literature in several important ways. Firstly, it broadens strategic assurance in internal auditing by identifying the operational pathways through which audit activity creates value beyond the governance and compliance function. Rather than treating financial risk auditing as a passive control device, the model positions it as an active organizational capability that influences production efficiency, cost management, quality performance, delivery reliability, and long-term sustainability. This perspective also reframes auditing as part of the broader architecture of performance management systems.

Secondly, the framework responds to the need for greater use of integrated approaches to performance management (Neely et al., 2005) by defining financial risk audit processes as strategic inputs into operational decision-making. Connecting financial governance with operations management, two areas that have historically developed independently of each other, highlights the interdependence between financial discipline and operational excellence. Risk intelligence generated through auditing does not merely reduce exposure; it informs resource allocation, process redesign, and strategic prioritization, thereby contributing to continuous improvement and performance optimization.

Thirdly, integrating the concept of organizational resilience into the analysis extends our understanding of industrial performance from the narrow perspective of short-term efficiency. Sustainable performance depends not only on cost control and productivity gains but also on the organization's capacity to anticipate disruptions, absorb shocks, and adapt to changing conditions. By using enhanced risk visibility as its informational mechanism, process modification as its corrective mechanism, and the development of risk-aware norms and a learning culture as its cultural mechanism, financial risk auditing strengthens this adaptive capacity and supports long-term competitiveness.

The proposed model greatly extends our understanding of the role of financial risk auditing in industrial performance beyond traditional compliance or control functions. From an agency theory perspective (Jensen & Meckling, 1976), financial risk auditing enables managers to be

held accountable for their actions through improved risk reporting, thereby reducing information asymmetry. From a resource-based view, knowledge produced by the audit function can be viewed as an intangible resource that assists in the operation of an organization and supports organizational learning. A dynamic capabilities perspective (Teece et al., 1997) posits that organizations integrating audit insights into decision-making processes and continuous improvement initiatives are better able to respond to environmental uncertainty and possible operational disruptions. Therefore, the mechanisms identified in the proposed framework demonstrate how financial risk auditing plays an important strategic role in enhancing both operational performance and an organization's long-term resilience.

From a managerial perspective, the framework underscores that the performance impact of financial risk auditing is contingent rather than automatic. Audit reports, suggestions, and risk evaluations create value if they fit into managers' everyday routines and operations. For audit practitioners, this entails producing outputs that are not only technically rigorous but also strategically aligned, clearly communicated, and operationally relevant. For industrial managers, this means integrating audit results into their production planning, inventory management, cost reduction, and process improvement efforts. For senior leadership, the findings emphasize the need to foster cross-functional integration, managerial commitment, and a mature risk culture that can translate audit findings into coordinated organizational action.

One of the fundamental objectives of this framework is to establish a coherent basis for understanding financial risk auditing as a strategic lever of industrial performance rather than merely a compliance-oriented control function. By clarifying the mechanisms, organizational conditions, and performance dimensions, and by contributing to theoretical integration, it offers concrete guidance to organizations seeking to align their governance structures with operational excellence and long-term resilience.

5. Conclusion

This article sought to fill a long-standing theoretical gap in the literature: the lack of a coherent framework for explaining how financial risk auditing translates into improvements in industrial performance. Through a structured, critical, and integrative review of research spanning financial risk management, strategic auditing, and industrial performance measurement, the study developed a conceptual model that clarifies the mechanisms underlying this relationship. The proposed framework is structured around three interconnected components—inputs, processes, and outcomes—and identifies three mediating mechanisms through which audit outputs influence performance. The informational mechanism enhances managerial decision-making by providing reliable, timely risk intelligence. The corrective mechanism translates

audit recommendations into targeted actions that address control weaknesses and process inefficiencies. The cultural and learning mechanisms increase the organization's awareness of risk and its ability to adjust to future risks, thus making it more resilient over time. Importantly, these mechanisms are not standalone; rather, they are interdependent and reinforce one another, forming a flexible process where audit activity leads to sustainable performance outcomes.

The framework advances the literature in several important respects. It broadens the strategic reassurance view of internal auditing by identifying the operational channels through which audit functions create value beyond governance and regulatory compliance requirements. More specifically, the study conceptualizes financial risk auditing as an indirect organizational capability that operates through informational, corrective, and cultural mechanisms to sustainably improve industrial performance. It bridges two research domains, financial governance and operations management, that have traditionally evolved in relative isolation, highlighting the interdependence between financial discipline and operational excellence. Furthermore, it integrates the concept of organizational resilience into the understanding of industrial performance, recognizing that sustainable success depends not only on efficiency gains but also on adaptive capacity.

From a managerial standpoint, this framework offers actionable implications. For auditors, it underscores the importance of making audit results available on demand, within the organization's defined delivery timeframe, and aligning them with the organization's operational priorities. For industrial managers, it highlights the need to integrate audit information in production planning, cost control, and continuous improvement efforts. For top management, the framework stresses the need to ensure that the strategic impact of auditing depends on cross-functional alignment, strong leadership commitment, and the development of a mature risk culture that transforms audit findings into coordinated organizational responses.

This study has certain limitations that should be acknowledged. As a primarily conceptual contribution based on an integrative literature review, the proposed framework has not yet been empirically validated. Consequently, the relationships between financial risk auditing and industrial performance remain theoretical and may vary across organizational and sectoral contexts.

In the future, researchers should operationalize the three proposed mediation mechanisms, develop reliable measurement tools to test the hypothetical relationships described in different industry contexts, and investigate the role of contextual factors such as sectoral nature, governance maturity, and digital transformation. Furthermore, as artificial intelligence and advanced data analytics techniques become more integrated into the audit process, there is

considerable potential to develop more predictive audit models that support organizational resilience.

In summary, this article considers financial risk auditing not only as a means of complying with regulatory requirements but also as a strategic organizational capability that enhances industrial performance and resilience in increasingly complex and high-risk environments. By clarifying the mechanisms and conditions under which audit activities contribute to operational results, this study offers researchers and practitioners a coherent perspective on and means to leverage the strategic value of financial risk auditing. Beyond enriching academic knowledge and management practices, this conceptual framework paves the way for theoretical developments and empirical validation, thereby promoting a sustainable industrial future for all organizations.

Reference:

- Argyris, C., & Schön, D. A. (1978). *Organizational learning: A theory of action perspective*. Addison-Wesley.
- Barney, J. B. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, 17(1), 99–120. <https://doi.org/10.1177/014920639101700108>
- Beasley, M. S., Clune, R., & Hermanson, D. R. (2005). Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy*, 24(6), 521-531. <https://doi.org/10.1016/j.jaccpubpol.2005.10.001>
- Brealey, R. A., Myers, S. C., & Allen, F. (2020). *Principles of corporate finance* (13th ed.). McGraw-Hill Education.
- Brigham, E. F., & Ehrhardt, M. C. (2020). *Financial management: Theory and practice* (16th ed.). Cengage Learning.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2004). *Enterprise Risk Management: Integrated Framework*. COSO.
- Eulerich, M., & Eulerich, A. (2020). What is the value of internal auditing? A literature review on qualitative and quantitative perspectives. *Maandblad voor Accountancy en Bedrijfseconomie*, 94(3/4), 83–92. <https://doi.org/10.5117/mab.94.50375>
- Florio, C., & Leoni, G. (2017). Enterprise risk management and firm performance: The Italian case. *The British Accounting Review*, 49(1), 56–74. <https://doi.org/10.1016/j.bar.2016.08.003>
- Gramling, A. A., Maletta, M. J., Schneider, A., & Church, B. K. (2004). The role of the internal audit function in corporate governance: A synthesis of the extant internal auditing literature and directions for future research. *Journal of Accounting Literature*, 23, 194–244.
- Hull, J. C. (2018). *Risk management and financial institutions* (5th ed.). Wiley.

- Jaakkola, E. (2020). Designing conceptual articles: Four approaches. *AMS Review*, 10(1), 18–26). <https://doi.org/10.1007/s13162-020-00161-0>
- Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305–360. [https://doi.org/10.1016/0304-405X\(76\)90026-X](https://doi.org/10.1016/0304-405X(76)90026-X)
- Lengnick-Hall, C. A., Beck, T. E., & Lengnick-Hall, M. L. (2011). Developing a capacity for organizational resilience through strategic human resource management. *Human Resource Management Review*, 21(3), 243–255. <https://doi.org/10.1016/j.hrmr.2010.07.001>
- Liu, Y., Li, R., & Wu, G. (2025). How does national audit affect enterprises' operating efficiency? *Finance Research Letters*, 85, 108065. <https://doi.org/10.1016/j.frl.2025.108065>
- Mautz, R. K., & Sharaf, H. A. (1961). *The philosophy of auditing*. American Accounting Association.
- Neely, A., Gregory, M., & Platts, K. (2005). Performance measurement system design: A literature review and research agenda. *International Journal of Operations & Production Management*, 25(12), 1228–1263. <https://doi.org/10.1108/01443570510633639>
- Power, M. (2007). *Organized uncertainty: Designing a world of risk management*. Oxford University Press
- Sarens, G., & De Beelde, I. (2006). The relationship between internal audit and senior management: A qualitative analysis of expectations and perceptions. *International Journal of Auditing*, 10(3), 219–241. <https://doi.org/10.1111/j.1099-1123.2006.00351.x>
- Saunders, A., & Cornett, M. M. (2018). *Financial institutions management: A risk management approach* (9th ed.). McGraw-Hill Education.
- Simons, R. (1995). *Levers of control: How managers use innovative control systems to drive strategic renewal*. Harvard Business School Press.
- Skinner, W. (1969). Manufacturing—Missing link in corporate strategy. *Harvard Business Review*, 47(3), 136–145.
- Slack, N. (1991). *The manufacturing advantage: Achieving competitive manufacturing operations*. Mercury Books.
- Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, 18(7), 509–533. [https://doi.org/10.1002/\(SICI\)1097-0266\(199708\)18:7%3C509::AID-SMJ882%3E3.0.CO;2-Z](https://doi.org/10.1002/(SICI)1097-0266(199708)18:7%3C509::AID-SMJ882%3E3.0.CO;2-Z)
- Institute of Internal Auditors. (2017). *International standards for the professional practice of internal auditing*. Institute of Internal Auditors.

***Chapitre 5: Communication managériale et communication des risques : vers
une gouvernance renouvelée à l'ère numérique***

Oumayma aït moussa

Docteure en sciences économiques et de gestion-oumaymaaitmoussa8@gmail.com

Chaymae YOUSFI

Docteure en sciences économiques et de gestion-chaymaeyousfi@hotmail.fr

Les processus de communication constituent un champ de recherche intrinsèquement interdisciplinaire. Ils ont suscité l'intérêt de disciplines aussi diverses que l'histoire, la géographie, la sociologie, la psychologie, les sciences politiques, l'économie, la biologie, la cybernétique ou encore les sciences cognitives (JOLY, 2009). Cette pluralité d'approches témoigne de la complexité du phénomène communicationnel, envisagé à la fois comme processus technique, interaction sociale et mécanisme structurant des organisations.

La notion de communication recouvre en effet une multiplicité de sens. Elle renvoie d'abord à l'action de communiquer, de transmettre et d'informer. Elle peut être appréhendée selon trois dimensions complémentaires : l'expression, lorsqu'il s'agit de manifester une intention, une émotion ou un état de conscience ; la représentation, lorsqu'elle vise à transmettre des connaissances ou à restituer des événements ; et l'action sur autrui, lorsqu'elle cherche à convaincre, influencer ou orienter les comportements. La communication déborde ainsi le cadre strictement verbal et mobilise une pluralité de signaux, mimiques, supports et technologies, notamment numériques. (JOLY, 2009).

Partant de ce constat, on peut dire que toute communication peut être conceptualisée comme un processus impliquant un émetteur qui transmet un message à un récepteur, via un canal, dans un environnement susceptible d'être perturbé par des « bruits » ou des obstacles altérant la compréhension. Cette représentation trouve une formalisation théorique majeure dans le modèle de Shannon et Weaver (1949), qui demeure l'un des cadres analytiques les plus influents pour appréhender les mécanismes fondamentaux de transmission de l'information.

Dans le champ des sciences de gestion, la communication ne constitue plus un simple outil périphérique. Elle devient progressivement la nouvelle frontière d'un management confronté à des défis organisationnels croissants, notamment en matière d'innovation, de coordination et de gestion des incertitudes (Maurice Imbert, 2015). En tant que processus, elle est indispensable tant pour la prise de décision que pour la diffusion et l'appropriation de ces décisions. Dès lors, la communication ne peut plus être envisagée comme un simple support aux logiques gestionnaires ; elle s'impose comme une composante centrale du management contemporain. Cette évolution est particulièrement manifeste dans le domaine de la gestion des risques, et plus spécifiquement des risques opérationnels. Longtemps appréhendée comme un mécanisme formel de remontée d'informations et de conformité aux cadres normatifs, la communication des risques tend aujourd'hui à s'affirmer comme un levier stratégique de gouvernance, notamment sous l'effet de la digitalisation des organisations et de l'intensification des exigences

réglementaires. (Committee of Sponsoring Organizations of the Treadway Commission [COSO], 2017 ; Basel Committee on Banking Supervision, 2011).

Dans ce contexte, notre problématique se pose ainsi : Dans quelle mesure la transformation numérique reconfigure-t-elle les dynamiques de communication managériale et de communication des risques au service d'une gouvernance organisationnelle renouvelée ?

Afin d'apporter des éléments de réponse à cette problématique, cet article propose une articulation du modèle de Shannon et Weaver avec le champ de la gestion des risques opérationnels, en analysant empiriquement les pratiques de communication au sein d'une institution bancaire. L'objectif est de montrer que la communication des risques ne se réduit pas à un transfert d'informations, mais qu'elle participe à la structuration d'une gouvernance renouvelée, fondée sur la qualité des flux informationnels, l'appropriation des messages par les acteurs et l'intégration des outils numériques.

L'article s'organise en trois parties : La première est consacrée à une revue de littérature structurée autour de deux axes : la communication au cœur de la transformation des pratiques de gestion des risques, ainsi que l'articulation entre communication managériale et communication des risques, afin de clarifier leurs interactions conceptuelles et organisationnelles. La deuxième partie présente la méthodologie adoptée, fondée sur une étude de cas qualitative reposant sur des entretiens semi-directifs et une analyse thématique de contenu. Enfin, la troisième partie expose les résultats empiriques et leur discussion, en mettant en évidence les apports du modèle de Shannon et Weaver à la compréhension des dynamiques communicationnelles des risques opérationnels et de leurs implications en matière de gouvernance à l'ère numérique.

1. Revue de littérature

1.1 La communication au cœur de la transformation des pratiques de gestion des risques

Depuis son apparition au début des années 1990, le cadre COSO (Committee of Sponsoring Organizations of the Treadway Commission) n'a cessé d'évoluer afin de répondre aux exigences croissantes en matière de gouvernance, de gestion des risques et de transparence organisationnelle. Parmi ses composantes structurantes, « Information et Communication » occupe une place singulière, car elle constitue le vecteur par lequel les dispositifs de contrôle interne et de gestion des risques deviennent opérationnels et partagés par les parties prenantes (COSO, 1992).

Le premier référentiel de 1992, dit COSO I, a introduit cinq composantes interdépendantes du contrôle interne, dont la communication. À ce stade, celle-ci est essentiellement envisagée comme un flux interne et externe d'informations pertinentes, fiables et en temps opportun, permettant d'assurer la circulation des directives managériales, le reporting financier et la remontée d'anomalies. La communication est encore perçue comme un support technique, garantissant la transmission d'informations nécessaires au bon fonctionnement du contrôle interne (Moeller, 2011).

Avec l'élargissement du modèle vers la gestion des risques d'entreprise en 2004, la composante « Information et Communication » prend une dimension plus stratégique. Il ne s'agit plus uniquement de diffuser des données, mais de permettre une communication transversale et ascendante entre les différents niveaux hiérarchiques, afin de favoriser une culture du risque partagée. Cette évolution consacre le rôle de la communication comme instrument de coordination et de cohérence dans les processus de gestion des risques (Frigo & Anderson, 2011).

La révision de 2013, souvent désignée comme COSO 2013, accorde une importance accrue à la qualité et à la traçabilité de l'information. La communication devient interactive et bidirectionnelle, intégrant les parties prenantes internes et externes. Le référentiel insiste également sur l'adaptation des canaux et des supports de communication aux besoins spécifiques des utilisateurs, renforçant ainsi la dimension de pertinence et de transparence. Cette étape reflète la montée en puissance des exigences réglementaires, notamment à la suite des crises financières de 2008, et des attentes accrues en matière de gouvernance d'entreprise (Kaplan, 2014).

Dans sa dernière version publiée en 2017, le cadre COSO met en avant cinq composantes essentielles de l'Enterprise Risk Management, parmi lesquelles « Information, Communication & Reporting » occupe une place centrale. Cette composante n'est plus conçue comme un simple mécanisme de transmission d'informations, mais comme un levier stratégique favorisant la transparence, la cohérence et l'intégration de la gestion des risques à la performance organisationnelle. Le modèle COSO ERM 2017, représenté ci-après, illustre cette nouvelle orientation en plaçant la communication au cœur de la gouvernance des risques et de la stratégie.

Enfin, la mise à jour de 2017, COSO ERM – *Integrating with Strategy and Performance*, marque un tournant décisif. Le volet « Information, Communication & Reporting » est érigé

comme pilier central du processus de gestion des risques intégrée à la stratégie et à la performance. La communication est ici perçue non seulement comme un outil de diffusion, mais comme un véritable levier de gouvernance, permettant de relier l'identification et l'évaluation des risques à la prise de décision stratégique. L'accent est également mis sur la digitalisation des flux d'information, l'utilisation d'outils analytiques avancés et la nécessité d'une communication transparente envers les investisseurs, les régulateurs et l'ensemble des parties prenantes (COSO, 2017 ; Beasley, Branson & Hancock, 2019).

Figure 1. Modèle COSO ERM (2017) – Les cinq composantes de la gestion des risques intégrée



Source: COSO, 2017, *Enterprise Risk Management – Integrating with Strategy and Performance*

La communication des risques constitue une dimension essentielle du dispositif de contrôle interne tel que promu par le référentiel COSO, il demeure nécessaire d'interroger la nature même de cette communication au sein des organisations. En effet, au-delà des prescriptions normatives, la transmission, l'interprétation et la compréhension des messages relatifs aux risques relèvent d'un processus de communication managériale plus large. Cette lecture ouvre la voie à une réflexion plus large sur les **interactions entre communication managériale et communication des risques**, et sur la manière dont ces deux dimensions contribuent conjointement à une gouvernance organisationnelle plus efficace.

1.2 Communication managériale et communication des risques : Quel rapport ?

La communication managériale peut être définie comme une communication de proximité portée par le manager afin de favoriser l'appropriation de la stratégie par ses collaborateurs (Imbert & Brouard, 2015). Traditionnellement, elle s'organise selon des axes verticaux (Imbert & Brouard, 2015) : la communication ascendante (remontée d'informations des opérationnels vers les dirigeants) et la communication descendante (diffusion de directives hiérarchiques). Cependant, les mutations contemporaines imposent une communication horizontale favorisant des relations d'égalité et de transversalité entre collaborateurs de même niveau hiérarchique (Mazzei, 2014 ; Heath & O'Hair, 2020). Dans le domaine des risques, la communication interne

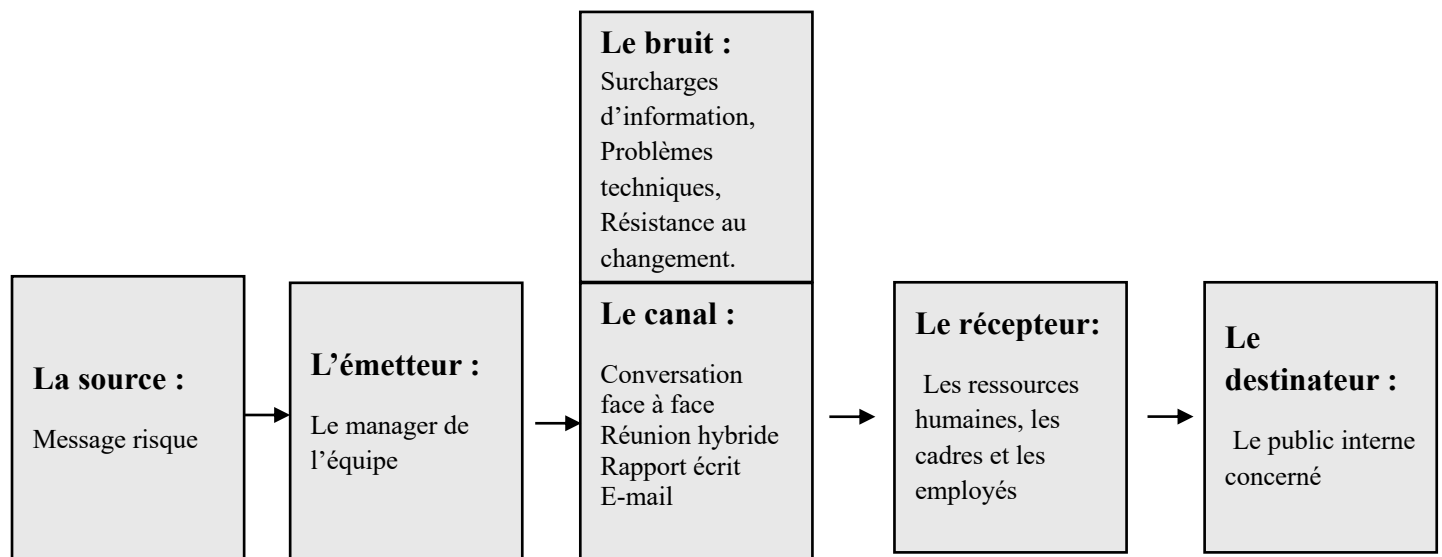
(politiques de gestion, remontées d'incidents, signaux faibles) s'articule ainsi de plus en plus avec une communication externe complexe (rapports prudentiels aux régulateurs, transparence aux investisseurs, gestion de la réputation médiatique) (Power, 2009 ; Hopkin, 2018).

Pour analyser ces flux, la littérature managériale a fréquemment mobilisé le modèle historique de Shannon et Weaver (1949). Issu des sciences de l'information et de la cybernétique, ce modèle linéaire conçoit la communication comme la reproduction exacte d'un message d'un point d'origine à un point de destination via une succession d'éléments : la source, l'émetteur (encodeur), le canal (support), le récepteur (décodeur), le destinataire, le tout soumis à des bruits (perturbations).

Adapté de manière classique au management, ce modèle se décline ainsi : la source (le message sur le risque), l'émetteur (le manager), le message (l'instruction), le canal (e-mail, face à face), le récepteur (les employés) et le bruit (surcharge informationnelle, résistance au changement).

Pour illustrer l'adaptation du modèle de Shannon et Weaver au contexte managérial, le schéma suivant synthétise les éléments présentés précédemment :

Figure n°2 : Modèle de communication Shannon et Weaver (1949)



Source : Élaborée par nous-mêmes à partir du schéma de Shannon et Weaver (1949).

Partant de cet exemple susmentionné, le schéma de Shannon et Weaver est adapté au management pour analyser la transmission de l'information au sein de l'organisation. Il permet de prendre en considération les obstacles courants dans les structures organisationnelles à savoir : la hiérarchie, la culture d'entreprise ou les contraintes technologiques. Ce schéma peut

également être enrichi pour illustrer les différents flux de la communication : ascendante, descendante et horizontale.

Ainsi, la diversité des formes de communication des risques témoigne de son rôle central dans le dispositif global de gouvernance. Une communication efficace, qu'elle soit interne ou externe, formelle ou informelle, préventive ou réactive, conditionne non seulement la circulation de l'information mais également la capacité de l'organisation à développer une véritable culture du risque et à préserver sa résilience.

Une présentation purement linéaire de ce modèle s'avère toutefois insuffisante pour saisir la complexité des organisations contemporaines, les sciences de la communication ayant largement démontré les limites de cette approche techno-mécanique (Fiske, 1990). Tout d'abord, le modèle initial souffre d'une absence originelle de feedback : conçu pour les télécommunications, il omet la rétroaction et réduit le récepteur à une entité passive alors qu'en gestion des risques, un collaborateur n'est pas un simple terminal de réception mais réinterprète et co-construit le sens du message. De plus, on constate une réduction sémantique du « bruit » qui, pour Shannon et Weaver, se limite à une perturbation technique du canal alors qu'en management, le bruit est essentiellement sémantique, psychologique et culturel, englobant les conflits d'objectifs, la peur de la sanction ou les logiques d'entraide locale. Enfin, ce cadre entretient l'illusion de la rationalisation technologique en laissant croire qu'il suffit d'optimiser le canal technique pour que l'information soit parfaitement transmise, ignorant ainsi les dynamiques relationnelles et émotionnelles qui caractérisent pourtant la communication de proximité.

Pourtant, à l'ère numérique, ces typologies et ces canaux traditionnels connaissent un renouvellement profond grâce à l'avènement des outils digitaux. Les plateformes collaboratives, les systèmes de reporting automatisés et les tableaux de bord dynamiques permettent d'accélérer la circulation des informations et de réduire les délais de réaction (Beasley, Branson & Hancock, 2019). L'analytique avancée, l'intelligence artificielle et les systèmes d'alerte en temps réel élargissent considérablement les capacités de détection et d'anticipation des risques (Chong & Shi, 2015). Par ailleurs, la communication externe s'appuie désormais sur les réseaux sociaux et les portails numériques institutionnels pour assurer une diffusion transparente et rapide des informations, tout en exigeant une vigilance accrue face aux risques réputationnels (Etter, Ravasi & Colleoni, 2019). L'enjeu conceptuel réside alors précisément dans cette tension : alors que la technologie numérise, automatise et prétend fluidifier les canaux pour éradiquer les défaillances techniques, elle accentue paradoxalement

les besoins d'une régulation managériale humaine pour surmonter les bruits sémantiques et comportementaux que les outils algorithmiques ne peuvent capter de manière isolée.

Pour dépasser ces limites et répondre à notre problématique, nous proposons un modèle conceptuel intégré. Ce modèle postule que la transformation numérique réorganise les canaux techniques de communication (progiciels, workflows), mais que l'efficacité réelle du dispositif de gouvernance dépend de l'articulation entre ces flux formels et la communication managériale de proximité. C'est au niveau des récepteurs (acteurs de terrain) que se jouent l'interprétation des messages et la gestion des bruits sémantiques (arbitrages entre respect strict de la norme et impératifs de performance commerciale).

2. Méthodologie

La présente recherche adopte une approche qualitative à visée compréhensive, particulièrement adaptée à l'étude des phénomènes organisationnels complexes et contextualisés. Selon Creswell (2013), les méthodes qualitatives permettent d'explorer en profondeur les significations, les perceptions et les pratiques des acteurs, ce qui correspond pleinement à l'objectif de compréhension des mécanismes de communication managériale des risques opérationnels dans un contexte de transformation numérique.

Sur le plan épistémologique, l'étude s'inscrit dans une posture interprétativiste, laquelle considère que la réalité organisationnelle est socialement construite à travers les interactions et les discours des acteurs (Burrell & Morgan, 1979). Cette posture est particulièrement pertinente pour analyser la communication des risques, envisagée non comme un simple transfert d'informations, mais comme un processus dynamique de construction du sens au sein de l'organisation.

Le cadre théorique mobilisé repose sur le modèle de communication de Shannon et Weaver (1949), initialement développé dans le champ de la théorie de l'information. Ce modèle, structuré autour des notions d'émetteur, de message, de canal, de récepteur et de bruit, a été largement mobilisé et adapté dans les sciences de gestion pour analyser les processus de communication organisationnelle (Fiske, 1990). Son articulation à la gestion des risques opérationnels permet d'examiner la fiabilité et l'efficacité de la transmission des informations liées aux risques, ainsi que les perturbations susceptibles d'altérer la qualité de la communication, notamment dans un environnement numérique.

D'un point de vue méthodologique, la recherche repose sur une étude de cas unique, conformément aux recommandations de Yin (2018), pour qui l'étude de cas constitue une stratégie pertinente lorsque l'on cherche à analyser un phénomène contemporain dans son contexte réel, en particulier lorsque les frontières entre le phénomène et le contexte ne sont pas clairement délimitées. Le terrain retenu est celui de la Banque Populaire, choisie en raison de la structuration de ses dispositifs de gestion des risques opérationnels et de l'intégration d'outils numériques dans ses processus de communication interne.

2.1 Méthode de collecte des données

La collecte des données empiriques s'est appuyée sur la conduite d'entretiens semi-directifs, méthode privilégiée dans les recherches qualitatives en management pour accéder au discours des acteurs et à leur expérience vécue (Kvale, 1996 ; Wacheux, 1996). Les entretiens ont été menés auprès de collaborateurs occupant différentes fonctions et niveaux hiérarchiques, impliqués dans la gestion ou la communication des risques opérationnels. Un guide d'entretien a été élaboré en amont, structuré autour des dimensions du modèle de Shannon et Weaver, tout en conservant une flexibilité suffisante afin de favoriser l'émergence de thèmes non préalablement identifiés.

Les données recueillies ont été intégralement retranscrites puis analysées à l'aide d'une analyse thématique de contenu, conformément aux travaux de Bardin (2013). L'analyse a suivi une double logique :

- Une logique déductive, fondée sur les catégories issues du cadre théorique mobilisé, et une logique inductive, permettant de faire émerger des dimensions nouvelles à partir du discours des acteurs. Cette démarche favorise une compréhension approfondie des pratiques de communication des risques et de leur contribution à une gouvernance organisationnelle renouvelée à l'ère numérique.
- Enfin, la validité de la recherche repose sur la cohérence entre le cadre théorique, la stratégie méthodologique et les outils de collecte et d'analyse des données. Conformément aux recommandations de Miles et Huberman (2003), une attention particulière a été portée à la saturation des données et à la confrontation des discours. Les résultats issus de cette étude de cas unique ne visent pas une généralisation statistique, mais une généralisation analytique, permettant d'enrichir la réflexion théorique sur la communication managériale des risques opérationnels dans les organisations bancaires.

2.2 Justification du choix de la Banque Populaire comme cas d'étude

Le choix de la Banque Populaire Régionale de l'Oriental en tant qu'étude de cas repose sur plusieurs critères stratégiques. En effet dans le cadre de sa stratégie globale de gestion des risques, la Banque Populaire s'aligne sur le Risk Assessment Statement (RAS) et le Risk Assessment Framework (RAF) élaborés par le Groupe BPCE. Ces cadres méthodologiques sont adaptés et déployés au sein de chaque établissement et filiale afin d'assurer la cohérence de l'identification, de l'évaluation, du suivi et du contrôle des risques opérationnels. La gestion de ces risques couvre l'ensemble des entités consolidées du Groupe, y compris les activités externalisées considérées comme essentielles ou significatives, conformément à la réglementation applicable (décret du 3 novembre 2014, modifié en 2021). La gouvernance est organisée à deux niveaux : d'une part, le Comité des risques non financiers Groupe (CRNFG), qui fixe les orientations stratégiques ; et, d'autre part, la Direction des risques opérationnels Groupe (DROG), chargée d'assurer la mise en œuvre opérationnelle de ces orientations.

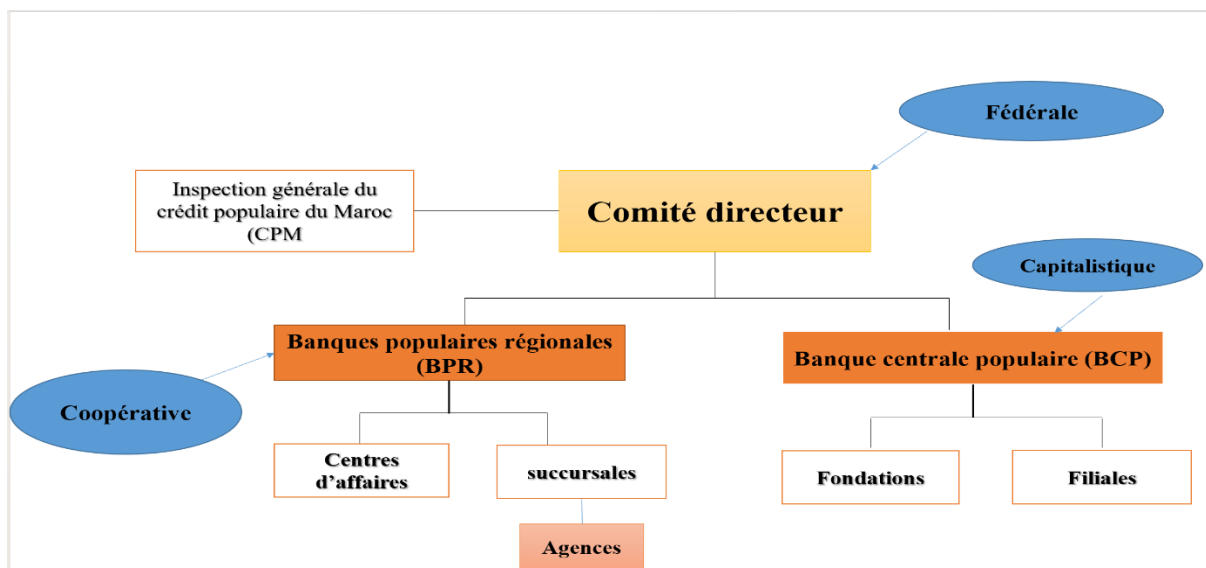
Chaque établissement dispose d'une Direction des risques opérationnels, appuyée par des correspondants métiers rattachés fonctionnellement à cette direction. Ces acteurs jouent un rôle clé dans le déploiement des outils du Groupe, le contrôle qualité des données enregistrées, le suivi des incidents, la mise à jour des indicateurs de risque et la préparation des reportings. Ils participent également au processus régulier de cartographie des risques ainsi qu'à la mise en œuvre des actions correctives validées en comité.

Plus spécifiquement, Banque Populaire Auvergne Rhône Alpes a mis en place un dispositif centralisé, appuyé par des comités trimestriels dédiés aux risques opérationnels, ainsi qu'une communication systématique à la direction générale en cas d'incidents majeurs. Le responsable des risques opérationnels y assure plusieurs fonctions essentielles : définition de la politique de gestion des risques, élaboration des procédures, évaluation des expositions et production des reportings de risque.

L'outil OSIRISK constitue la pierre angulaire du dispositif opérationnel. Il permet une évaluation continue des risques, la gestion des incidents, l'actualisation régulière de la cartographie des risques et le suivi des plans d'action. Cet outil soutient une démarche prospective intégrant les risques émergents, les menaces liées aux technologies de l'information et à la cybersécurité, ainsi que les risques associés aux prestataires tiers et à la non-conformité réglementaire.

Enfin, la banque s'appuie sur un tableau de bord des risques opérationnels mis à jour trimestriellement, ainsi que sur un système de reporting alimenté par un data smart interne. Pour le calcul de ses exigences en fonds propres, le Groupe BPCE applique l'approche standardisée prévue par le cadre réglementaire de Bâle II. Structure organisationnelle mixte : Son modèle de gouvernance combine une autonomie régionale avec une centralisation stratégique.

Figure 3. Structure organisationnelle de l'étude de cas « Crédit Populaire du Maroc ».



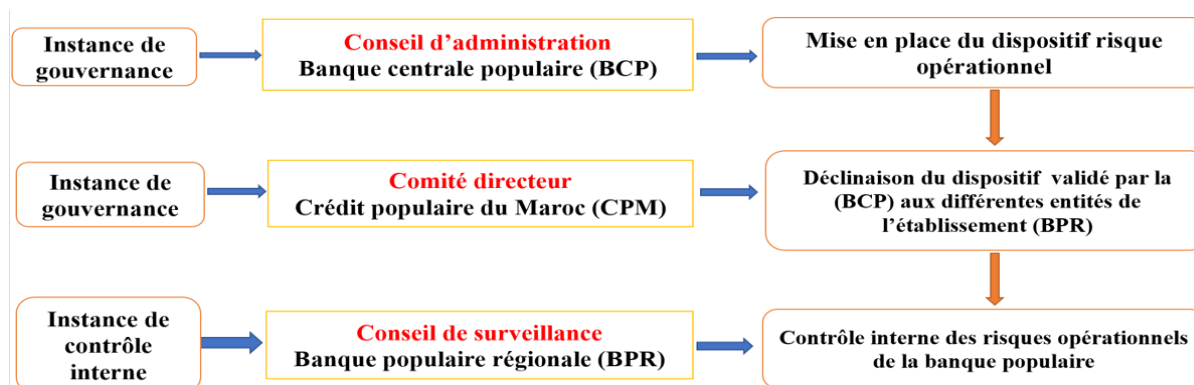
Source : Élaborée par les auteurs.

Le premier schéma met en évidence la structure fédérative du Crédit Populaire du Maroc (CPM), organisée autour d'un Comité de direction, organe central de gouvernance, placé sous la supervision de l'Inspection générale du Crédit Populaire du Maroc. Cette structure hybride combine deux logiques : une logique coopérative et une logique capitaliste.

La branche coopérative est représentée par les Banques Populaires Régionales (BPR), entités autonomes opérant au niveau local. Elles assurent une proximité étroite avec la clientèle grâce à un réseau de centres d'affaires, de succursales et d'agences.

Parallèlement, la branche capitaliste est incarnée par la Banque Centrale Populaire (BCP), institution faîtière du groupe. Elle joue un rôle clé dans la planification stratégique, la coordination et la gestion des filiales et des fondations. Cette dualité entre logique régionale et gouvernance centralisée constitue un mécanisme d'équilibre entre l'ancrage local et la supervision globale.

Figure 4. Gouvernance du risque opérationnel – Crédit Populaire du Maroc



Source : Élaborée par les auteurs.

Le second schéma illustre les différents organes de gouvernance et de contrôle interne impliqués dans la mise en œuvre et le suivi du dispositif de gestion des risques opérationnels.

Au niveau central, le Conseil d'administration de la BCP constitue l'organe de gouvernance stratégique chargé de concevoir et de déployer le cadre de gestion des risques opérationnels. Ce cadre est ensuite opérationnalisé par le Comité de direction du CPM, qui veille à traduire les orientations stratégiques en actions concrètes au sein des différentes entités du groupe, notamment les Banques Populaires Régionales (BPR).

Au niveau régional, les Conseils de surveillance des BPR représentent les organes de contrôle interne responsables de veiller à la bonne application des systèmes de gestion des risques. Cela inclut le suivi des risques opérationnels, selon une approche adaptée aux spécificités locales.

2.3 Méthode de collecte et d'analyse des données

Les données empiriques ont été collectées dans le cadre d'une étude de cas menée auprès de la Banque Populaire, choisie pour la structuration de son dispositif de gestion et de communication des risques opérationnels. Les entretiens ont été réalisés auprès d'acteurs clés impliqués dans ce dispositif (Risk Manager, auditeur interne, responsable correspondant risque opérationnel, correspondants risque opérationnel, chefs de succursales et chefs d'agences). Afin de garantir l'anonymat, chaque participant a été codifié par une lettre (A à F), utilisée lors de l'analyse des résultats.

Tableau n°1 : liste des interviewés

Code Acteur	Fonction de l'Interviewé	Nombre de Participants	Mode de Conduite	Durée Moyenne
A	Risk Manager	1	Présentiel (Siège)	65 min

B	Auditeur interne	1	Présentiel (Siège)	50 min
C	Responsable Correspondant Risque Opérationnel (RCRO)	1	Présentiel (Siège)	60 min
D	Correspondant Risque Opérationnel (CRO)	1	Présentiel (Siège)	45 min
E	Chef de Succursale	2	Présentiel (En Agence)	55 min
F	Chef d'Agence	2	Présentiel (En Agence)	45 min
Total	Acteurs interrogés	8 entretiens	-	53 min (Moy.)

Source : Élaborée par les auteurs.

Le recours aux **entretiens semi-directifs** se justifie par la nature exploratoire de la recherche et par la nécessité de comprendre les pratiques et perceptions des acteurs organisationnels. Comme le soulignent Blanchet et Gotman (1992), l’entretien constitue un outil privilégié lorsqu’il s’agit d’explorer un phénomène encore peu documenté empiriquement. Conformément à la typologie proposée par Wacheux (1996), la forme semi-directive a été retenue afin d’assurer un équilibre entre structuration thématique et liberté d’expression.

Le guide d’entretien a été élaboré à partir du cadre théorique mobilisé, fondé sur le modèle de Shannon et Weaver (1949), et structuré selon une progression « en entonnoir » (Gavard-Perret et al., 2008). Il visait à analyser les composantes du processus communicationnel (émetteur, message, canal, récepteur, bruit) appliquées à la gestion des risques opérationnels dans un environnement numérique.

Les entretiens ont été intégralement retranscrits et soumis à une **analyse thématique de contenu** selon les principes de Bardin (2013). L’analyse a combiné une logique déductive, fondée sur les catégories issues du modèle théorique, et une logique inductive permettant l’identification de dimensions émergentes liées à la digitalisation et à la gouvernance des risques.

Cette démarche permet d’appréhender la communication des risques opérationnels non seulement comme un processus de transmission d’information, mais comme un levier structurant d’une gouvernance organisationnelle renouvelée à l’ère numérique.

3. Analyse des résultats

Cette partie est consacrée à la présentation des résultats issus de l'analyse thématique de contenu réalisée à partir des huit entretiens conduits auprès des acteurs impliqués dans la gestion et la communication des risques opérationnels.

Ces entretiens avaient pour objectif d'apporter un éclairage qualitatif aux principales dimensions structurant notre problématique, à savoir : les composantes du processus de communication des risques opérationnels (émetteur, message, canal, récepteur), les sources de perturbation ou de « bruit » susceptibles d'altérer la transmission de l'information, ainsi que les implications de ces dynamiques communicationnelles en matière de gouvernance à l'ère numérique.

Nous présentons dans ce qui suit les résultats de l'analyse en les organisant autour de ces différentes dimensions, issues de l'articulation du modèle de Shannon et Weaver (1949) avec le champ de la gestion des risques opérationnels.

Pour chaque axe, l'interprétation des résultats repose sur une confrontation progressive entre les apports de la revue de littérature et les discours des répondants. Cette démarche analytique, combinant logique déductive (fondée sur le cadre théorique mobilisé) et logique inductive (fondée sur les éléments émergents du terrain), a permis de dégager un fil conducteur structurant la compréhension du phénomène étudié.

Ainsi, l'analyse met en évidence que la communication des risques opérationnels ne peut être réduite à un simple mécanisme de transmission d'information ; elle s'inscrit dans un processus organisationnel plus large, où la qualité des flux informationnels, la digitalisation des canaux et l'appropriation des messages par les acteurs contribuent à façonner les contours d'une gouvernance renouvelée.

3.1 Articulation avec le modèle de Shannon & Weaver

Ce modèle de communication appliqué à la gestion des risques opérationnels met en évidence les limites possibles du dispositif informationnel, notamment la sous-déclaration des incidents ou la dilution des messages de prévention. Il souligne l'importance d'une boucle de rétroaction efficace et d'une culture du risque partagée à tous les niveaux hiérarchiques.

Tableau n°2: Modélisation de la circulation de l'information sur le risque opérationnel à l'ère numérique selon le modèle de Shannon & Weaver

Élément du modèle	Application au flux de communication du risque	Exemple concret (Banque cas d'étude)
Émetteur	Direction Générale / entité opérationnelle / service transversal	Comité directeur (centrale)
Message	Politique risque opérationnel	Comité directeur : les grandes orientations stratégiques de gestion des risques au conseil d'administration au niveau national
Canal	Intranet, mail, réunion, workflow	Réunion des comités d'audit et des risques au niveau central en vue de la validation des orientations, puis de leur déclinaison via le système intranet propre à la banque.
Récepteur	Collaborateurs, direction, comités	Conseil d'administration veille à l'application des orientations générales du Comité Directeur Comité Gestion des risques et de la conformité : s'assure de l'application des orientations stratégiques arrêtées par le Comité Directeur Comité Audit : chargé de suivi de l'activité de l'audit interne et externe de la BCP et des filiales, ainsi que des recommandations de l'inspection générale du CPM
Bruit	Interprétation, surcharge d'info, réticence à signaler	Conseil de surveillance au niveau régional : Gestion et remontée des risques opérationnels à la centrale

Source : Elaborée par les auteurs.

Bien que le modèle de Shannon et Weaver offre une lecture structurée des flux d'information liés au risque opérationnel (émission, canal, réception, bruit), il reste réducteur dans le contexte managérial contemporain. En effet, la communication des risques ne se limite plus à une simple transmission d'informations : elle s'inscrit dans des dynamiques sociales, émotionnelles et numériques qui transforment les messages, les canaux et les perceptions.

3.2 La Gestion du risque au niveau de la banque populaire

La remontée de l'information liée aux risques opérationnels au sein de la Banque Populaire repose sur une articulation tripartite :

- **Les acteurs** : le dispositif mobilise un ensemble d'intervenants, allant de la superstructure (niveau décisionnel) à l'infrastructure (niveau opérationnel).
- **Les outils** : deux principales plateformes sont utilisées « *Paradigme* », dédiée aux acteurs de l'infrastructure, et *Front Risk*, destinée aux acteurs de la superstructure.
- **Les interactions** : elles se traduisent par une répartition précise des rôles et responsabilités dans le processus de déclaration et de gestion des risques.

La communication descendante, dictée par les exigences de conformité et de transparence (Bâle II, circulaire de Bank Al-Maghrib), s'appuie sur des dispositifs numériques visant à uniformiser le reporting. « *Nos chefs d'agences et succursales sont amenés à remonter l'incident une fois constatée pour qualification de l'événement* **Répondant C** ».

Toutefois, cette rationalisation technologique tend parfois à occulter les facteurs humains réticence à signaler les incidents, interprétation différenciée des risques, surcharge informationnelle qui génèrent un bruit communicationnel au sens de Shannon. Les résultats de l'analyse transversale du contenu des entretiens avec les chefs d'agences/ succursales nous ont révélé l'orientation des réponses vers deux perspectives différentes :

Pour le cas du chef d'agence « A » celui-ci privilégie l'option de remonté à la hiérarchie tout risque détecté, ce dernier est convaincu que la gestion des situations risquées ne peut se faire qu'en respectant les normes. « *Il n'incombe pas à moi de trouver des solutions pour les risques détectés, la politique de notre banque nous stipule de déclarer et remonter tout type de risque...* **Répondant D** ». Alors que pour d'autres chefs d'agence, ces derniers optent pour des solutions au niveau local afin de gérer les risques détectés « *on est avant tout là pour s'entraider et faire en sorte que les objectifs de la banque soient atteints, pour cela une fois un risque détecté on cherche à trouver les solutions possibles pour le surpasser,* **Répondant F** ».

Suite à ces entrevues susmentionnées, on peut résumer que la communication du risque opérationnel s’articule selon trois flux :

- Descendante, pour la diffusion des politiques et procédures édictées par la direction générale conformément aux exigences de Bâle et à la circulaire de Bank Al-Maghrib;
- Ascendante, à travers la remontée d’incidents via un workflow informatisé alimentant la cartographie des risques ;
- Transversale, qui favorise la coordination entre la direction des risques, le risk manager, les correspondants risque opérationnel et l’auditeur interne.

Le tableau ci-dessous synthétise ces dynamiques croisées :

Tableau 3. Matrice de synthèse des flux, bruits et impacts sur la gouvernance.

Flux de Communication	Canal Principal	Type de Message	Bruit Sémantique Identifié	Impact sur la Gouvernance
Descendant	Intranet / Workflows / Directives	Normes Bâle II / Procédures prudentielles	Surcharge informationnelle/ sentiment de surveillance managériale accrue	Uniformisation des procédures mais risque de rejet passif.
Ascendant	Plateforme OSIRISK / Front Risk	Déclaration d'incidents / Signaux faibles	Réticence à signaler / peur de la sanction	Cartographie des risques potentiellement biaisée ou décalée.
Transversal Horizontal	Réunions de proximité / Échanges directs	Entraide opérationnelle / Solutions locales	Opacité vis-à-vis de la superstructure	Résolution rapide des problèmes mais sous-déclaration systémique.

Source : Elaborée par les auteurs.

L'analyse de ces résultats confirme que la transformation numérique, bien qu'elle fournisse des canaux d'accélération informationnelle (Beasley et al., 2019), ne peut s'affranchir d'une animation managériale. Si les managers locaux (Répondant F) masquent le risque pour préserver l'atteinte des objectifs commerciaux, l'outil numérique fait l'objet d'un découplage et subit une perte de sens fonctionnel. Le défi d'une gouvernance renouvelée consiste donc à transformer ce « bruit » (la peur de déclarer) en une boucle de rétroaction positive grâce à une culture managériale non punitive du risque.

Conclusion

Au terme de cette analyse, il apparaît que la compréhension des dynamiques communicationnelles constitue un levier essentiel pour repenser la gouvernance des risques à l’ère numérique. Le schéma, inspiré du modèle de Shannon et Weaver, permet de visualiser les flux d’information relatifs au risque opérationnel au sein de la banque étudiée. Toutefois, à l’ère de la digitalisation, cette lecture linéaire révèle ses limites. La communication du risque ne peut plus être appréhendée comme un simple transfert de messages entre émetteurs et récepteurs ;

elle s'inscrit désormais dans un écosystème humain, organisationnel et technologique au sein duquel les significations se co-construisent. Ainsi, concilier les exigences normatives de transparence avec la dynamique humaine propre à la communication managériale constitue aujourd'hui un enjeu central pour la gouvernance bancaire. La communication contemporaine ne se limite plus à un modèle linéaire classique ; elle s'inscrit dans une logique de gouvernance renouvelée, fondée sur une circulation multidirectionnelle de l'information, intégrant des flux ascendants, descendants et horizontaux.

Sur le plan théorique, cette démarche enrichit les sciences de gestion en opérationnalisant le modèle de Shannon et Weaver au-delà de sa fonction cybernétique originelle. En le confrontant au cadre COSO ERM 2017, la recherche démontre que le concept de « bruit » en organisation n'est pas un simple défaut technique du canal, mais une construction sémantique et comportementale intimement liée aux structures de pouvoir, aux arbitrages de performance commerciale et à la culture d'entreprise.

Sur le plan pratique, ces résultats soulignent pour les dirigeants et Risk Managers l'illusion du « tout-technologique ». Déployer des plateformes de pointe comme OSIRISK s'avère inefficace si la ligne managériale intermédiaire perçoit le signalement d'incidents comme un outil de sanction ; il est donc impératif de coupler les outils de workflow avec des espaces de communication horizontale et une culture managériale bienveillante favorisant la transparence tout en brisant les silos informationnels.

Enfin, bien que la principale limite de cette recherche réside dans sa méthodologie qualitative ancrée sur une étude de cas unique à la Banque Populaire ce qui restreint la généralisation universelle des résultats au profit d'une transférabilité analytique, elle ouvre des voies de recherche futures stimulantes. Les travaux futurs pourraient ainsi explorer la nature des formations managériales nécessaires pour accompagner la digitalisation des outils, afin de comprendre comment développer chez les encadrants de proximité des compétences de communication favorisant une culture de transparence du risque.

Bibliographie

Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of Enterprise Risk Management. *Accounting, Organizations and Society*, 35(7), 659–675.

Bardin, L. (2013). *L'analyse de contenu* (2^e éd.). Presses Universitaires de France.

Beasley, M. S., Branson, B. C., & Hancock, B. V. (2019). Developing key risk indicators to strengthen enterprise risk management. *COSO Thought Leadership Report*. Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Beasley, M., Branson, B., & Hancock, B. (2019). The state of risk oversight: An overview of enterprise risk management practices. North Carolina State University.

Blanchet, A., & Gotman, A. (1992). *L'enquête et ses méthodes : L'entretien*. Nathan.

- Burrell, G., & Morgan, G. (1979). *Sociological paradigms and organisational analysis: Elements of the sociology of corporate life*. Heinemann.
- Chong, A. Y.-L., & Shi, C. (2015). A study of the impact of cloud computing on enterprise risk management. *International Journal of Information Management*, 35(6), 703–710. <https://doi.org/10.1016/j.ijinfomgt.2015.07.004>
- Chong, A. Y. L., & Shi, Y. (2015). Big data analytics: A review of techniques and applications in risk management. *Decision Support Systems*, 79.
- Coombs, W. T. (2014). *Ongoing crisis communication: Planning, managing, and responding*. Sage.
- COSO. (1992). *Internal control – Integrated framework*. Committee of Sponsoring Organizations of the Treadway Commission.
- COSO. (2004). *Enterprise risk management – Integrated framework*. Committee of Sponsoring Organizations of the Treadway Commission.
- COSO. (2013). *Internal control – Integrated framework*. Committee of Sponsoring Organizations of the Treadway Commission.
- COSO. (2017). *Enterprise risk management – Integrating with strategy and performance*. COSO & PwC.
- Creswell, J. W. (2013). *Qualitative inquiry and research design: Choosing among five approaches* (3rd ed.). Sage Publications.
- Etter, M., Ravasi, D., & Colleoni, E. (2019). Social media and the formation of organizational reputation. *Academy of Management Review*, 44(1), 28–52. <https://doi.org/10.5465/amr.2014.0280>
- Fiske, J. (1990). *Introduction to communication studies* (2nd ed.). Routledge.
- Frandsen, F., & Johansen, W. (2017). *Organizational crisis communication: A multivocal approach*. Sage.
- Frigo, M., & Anderson, R. (2011). What is strategic risk management? *Strategic Finance*.
- Gavard-Perret, M.-L., Gotteland, D., Haon, C., & Jolibert, A. (2008). *Méthodologie de la recherche en sciences de gestion : Réussir son mémoire ou sa thèse*. Pearson Education.
- Heath, R. L., & O’Hair, H. D. (Eds.). (2020). *Handbook of risk and crisis communication*. Routledge.
- Heurley, L. (2013). *La théorie mathématique de la communication (théorie de l'information) et la psychologie cognitive*. UFR Sciences Humaines, Sociales et Philosophie.

- Hopkin, P. (2018). *Fundamentals of risk management: Understanding, evaluating and implementing effective risk management* (5th ed.). Kogan Page.
- Imbert, M., & Brouard, V. (2015). *La communication managériale*. Dunod.
- Joly, B. (2009). *La communication*. De Boeck.
- Kaplan, R. S. (2014). Improving risk management: From processes to people. *Accounting Horizons*, 28(3).
- Kvale, S. (1996). *InterViews: An introduction to qualitative research interviewing*. Sage Publications.
- Mazzei, A. (2014). Internal communication for employee enablement: Strategies in American and Italian companies. *Corporate Communications: An International Journal*, 19(1), 82–95. <https://doi.org/10.1108/CCIJ-08-2012-0060>
- Miles, M. B., & Huberman, A. M. (2003). *Analyse des données qualitatives* (2^e éd.). De Boeck.
- Moeller, R. (2011). *COSO Enterprise Risk Management: Establishing effective governance, risk, and compliance*. Wiley.
- Power, M. (2009). The risk management of nothing. *Accounting, Organizations and Society*, 34(6–7), 849–855. <https://doi.org/10.1016/j.aos.2009.06.001>
- Rapport d'activité groupe banque populaire 2024
- Roy, C. (1995, 12 juin). Communication. Dans *Bidon, Tolérance* (p. 29).
- Shannon, C. E., & Weaver, W. (1949). *The mathematical theory of communication*. University of Illinois Press.
- Wacheux, F. (1996). *Méthodes qualitatives et recherche en gestion*. Economica.
- Weick, K. E., & Sutcliffe, K. M. (2015). *Managing the unexpected: Sustained performance in a complex world*. Wiley.
- Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). Sage Publications.

CHAPITRE 6: *La stratégie Leagile face aux risques logistiques : une étude empirique marocaine*

Kaoutar LAMAIZI. Doctorante

Laboratoires d'Études et Recherches Appliquées en Sciences Économiques (LERASE)
FSJES, Université Ibnou Zohr- Agadir, Maroc- kaoutar.lamaizi.68@edu.uiz.ac.ma

Amina KADA. Maître de conférences Habilité

Laboratoires d'Études et Recherches Appliquées en Sciences Économiques (LERASE)
Faculté Polydisciplinaire, Université Ibnou Zohr-Taroudant, Maroc- a.kada@uiz.ac.ma

Les chaînes logistiques industrielles évoluent dans un environnement caractérisé par une incertitude croissante et une exposition permanente à des risques multiformes. Dans un contexte mondial où la disruption est devenue la norme plutôt que l'exception, la capacité à gérer ces risques de manière proactive et adaptative constitue un avantage compétitif décisif. La crise sanitaire mondiale de 2020-2021 a particulièrement mis en exergue la vulnérabilité des systèmes logistiques face à des perturbations de grande ampleur, provoquant des ruptures d'approvisionnement en cascade et forçant les organisations à repenser fondamentalement leurs stratégies de gestion des risques (Ivanov & Dolgui, 2021 ; Queiroz et al., 2020). Mais au-delà de ces chocs exceptionnels, ce sont les perturbations ordinaires (pannes d'équipements, aléas de transport, dysfonctionnements de coordination, fluctuations des stocks, incidents humains) qui constituent le quotidien des responsables logistiques et pèsent le plus lourdement sur la performance opérationnelle (Chopra & Sodhi, 2004 ; Tang, 2006).

La littérature managériale a progressivement développé deux paradigmes complémentaires pour y répondre. Le Lean Management offre des leviers de stabilisation et de prévention (Womack & Jones, 1996), tandis que l'agilité organisationnelle renforce la capacité d'absorption face aux perturbations imprévues (Christopher, 2000 ; Teece et al., 2016). Ces deux approches, longtemps pensées comme antagonistes, ont été progressivement intégrées dans la stratégie Leagile, qui propose leur hybridation selon la nature des flux et des risques à gérer (Mason-Jones, Naylor & Towill, 2000 ; Tortorella et al., 2020).

Si la stratégie Leagile a suscité un intérêt croissant depuis les travaux fondateurs de Naylor, Naim et Berry (1999), sa contribution spécifique à la réduction des risques logistiques reste insuffisamment documentée empiriquement, particulièrement dans les contextes des pays en développement. Cette lacune est d'autant plus significative que les organisations marocaines font face à des configurations de risques singulières, liées à leurs infrastructures, à leurs écosystèmes logistiques et à leurs modes de gouvernance (Lavastre, Gunasekaran & Spalanzani, 2012 ; Sarkis et al., 2020).

Ce chapitre vise à combler partiellement ce vide en répondant à la question centrale suivante : comment la stratégie Leagile contribue-t-elle à la réduction des risques logistiques dans un environnement industriel où les flux sont continus, critiques et soumis à des aléas fréquents ? En réponse, nous proposons un cadre intégrateur original modélisant la dynamique Leagile de gestion des risques. Le chapitre est structuré en six sections couvrant successivement la revue de littérature et le cadre théorique, la méthodologie, les résultats, la discussion et la conclusion.

2. Revue de littérature et cadre théorique

2.1 Les risques logistiques : définition, nature et typologies

Le risque logistique désigne la probabilité qu'un événement perturbateur affecte négativement les flux physiques, informationnels ou financiers d'une chaîne logistique, compromettant la continuité des opérations et la satisfaction des parties prenantes (Zsidisin, 2003 ; Jüttner, Peck & Christopher, 2003). Chopra et Sodhi (2004) distinguent neuf catégories de risques logistiques (perturbations, délais, défaillances systèmes, erreurs de prévisions, risques d'approvisionnement, déséquilibres des inventaires et insuffisances de capacité), chacune appelant des stratégies de mitigation distinctes. Kleindorfer et Saad (2005) proposent une articulation complémentaire selon la source du risque, opérationnelle ou exogène. Plus récemment, Ivanov (2022) a introduit la notion de risques de « viabilité », menaçant l'existence même de la chaîne logistique, tandis qu'Ivanov et Dolgui (2021) soulignent l'émergence de risques numériques comme menace structurelle croissante à l'ère d'Industry 4.0.

Dans le contexte industriel, Lavastre, Gunasekaran et Spalanzani (2012) identifient quatre familles récurrentes : défaillances d'équipements, aléas de transport, dysfonctionnements de gestion des stocks et risques liés aux ressources humaines. Cette taxonomie, confirmée dans les pays émergents (Sarkis et al., 2020), guidera notre analyse empirique. La gestion de ces risques implique des démarches proactives (anticipation, prévention, standardisation) et réactives (mitigation, adaptation, rétablissement) (Tang, 2006). Cette dualité constitue précisément la valeur ajoutée de la stratégie Leagile.

2.2 Lean Management, agilité organisationnelle et stratégie Leagile

Le Lean Management, issu du Toyota Production System (Womack & Jones, 1996 ; Liker, 2004), vise l'élimination des gaspillages et la stabilisation des processus par la standardisation, la maintenance préventive (TPM), le management visuel et l'amélioration continue. Sur le plan empirique, Shah et Ward (2007), à partir d'une analyse de 313 établissements manufacturiers, démontrent que les pratiques Lean réduisent significativement la variabilité opérationnelle, principal vecteur de risques récurrents. Cependant, les systèmes très Lean présentent une vulnérabilité documentée : leur efficience repose sur la régularité des flux, ce qui les rend sensibles aux perturbations soudaines (Towill & Christopher, 2002). La pandémie de Covid-19 a dramatiquement illustré cette limite (Ivanov & Dolgui, 2021) : le Lean stabilise et prévient, mais ne suffit pas structurellement à absorber l'imprévisible.

L'agilité organisationnelle désigne la capacité d'une organisation à percevoir les signaux de changement et à y répondre rapidement en mobilisant des ressources flexibles et des processus reconfigurables (Gunasekaran, 1999 ; Christopher, 2000 ; Teece, Peteraf & Leih, 2016). Les pratiques agiles incluent la polyvalence des équipes, la constitution de capacités de réserve, la décentralisation décisionnelle et le partage de données en temps réel (Naylor, Naim & Berry, 1999 ; Christopher & Towill, 2001). Elles renforcent la résilience organisationnelle, définie par Ponomarov et Holcomb (2009) comme la capacité adaptative d'une chaîne logistique à se préparer aux perturbations, à y répondre et à s'en remettre. Chowdhury et Quaddus (2017), dans une recherche mixte auprès d'entreprises manufacturières australiennes, valident une échelle de mesure de la résilience fondée sur la théorie des capacités dynamiques, établissant que les organisations dotées de telles capacités présentent une résilience significativement supérieure. Brusset et Teller (2017), à partir d'une enquête auprès de 171 managers testée par équations structurelles, montrent que l'intégration inter-niveaux et la flexibilité constituent les deux leviers décisifs de la résilience opérationnelle.

La stratégie Leagile, formalisée par Mason-Jones, Naylor et Towill (2000) autour du modèle du point de découplage, hybride ces deux paradigmes : en amont, des pratiques Lean optimisent l'efficacité ; en aval, des pratiques agiles maximisent la réactivité. Krishnamurthy et Yauch (2007) ont étendu ce modèle au-delà des stocks pour montrer que le Leagile constitue un avantage organisationnel global. En matière de gestion des risques, cette configuration offre une réponse structurée à leur dualité fondamentale : le Lean traite les risques prévisibles par prévention et standardisation, l'agilité traite les risques imprévisibles par flexibilité et réactivité (Christopher & Towill, 2001 ; Rossini et al., 2019 ; Tortorella et al., 2020). La Figure 1 illustre ce modèle fondateur et son extension à la dynamique de résilience logistique.

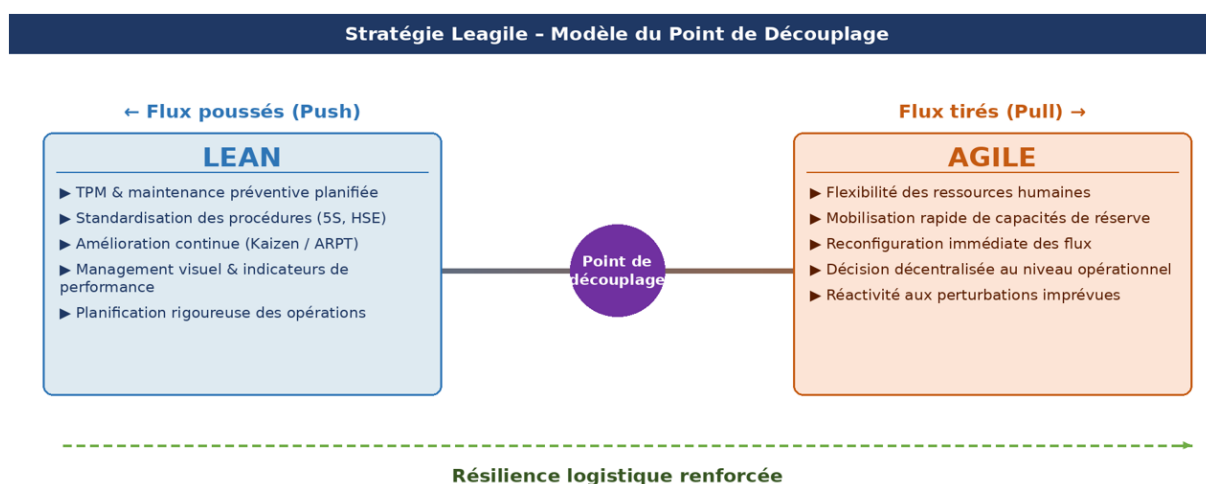


Figure 1 : Modèle du point de découplage Leagile et contribution à la résilience logistique

Source : Adapté de Mason-Jones, Naylor et Towill (2000) et Naylor et al. (1999), enrichi par les autrices.

Il convient néanmoins de souligner une limite de la littérature existante : la majorité des travaux empiriques sur le Leagile demeurent centrés sur la gestion des stocks et les flux physiques, négligeant les dimensions de coordination inter-services, de gestion des ressources humaines et de culture organisationnelle comme vecteurs de résilience. Notre étude vise précisément à documenter ces dimensions dans le contexte industriel marocain, encore sous-représenté dans la littérature internationale.

La revue de littérature permet de dégager trois constats structurants. Premièrement, les risques logistiques présentent une dualité fondamentale, prévisibles/récurrents versus imprévisibles/soudains, appelant des réponses différenciées (Chopra & Sodhi, 2004 ; Tang, 2006). Deuxièmement, Lean et agilité constituent des compétences complémentaires dont l'hybridation Leagile maximise la couverture des risques : la maturité Lean crée les conditions d'une agilité plus robuste, tandis que l'agilité confère au Lean la flexibilité qui lui fait structurellement défaut (Mason-Jones et al., 2000 ; Towill & Christopher, 2002). Troisièmement, cette hybridation n'est pas statique : l'apprentissage organisationnel constitue le mécanisme par lequel la configuration Leagile se renforce dans le temps (Tortorella et al., 2020 ; Chowdhury & Quaddus, 2017).

Sur la base de ces constats, deux propositions de recherche testables sont formulées :

P1 : Plus la maturité des pratiques Lean d'une organisation industrielle est élevée, plus sa capacité agile de réponse aux perturbations logistiques imprévues est efficace (Shah & Ward, 2007 ; Tortorella et al., 2020).

P2 : La présence de pratiques hybrides spontanées combinant Lean et Agile dans les équipes opérationnelles est positivement associée à la résilience logistique organisationnelle, mesurée par la réduction des temps de rétablissement post-perturbation (Brusset & Teller, 2017 ; Chowdhury & Quaddus, 2017).

3. Méthodologie de recherche

3.1 Positionnement épistémologique et terrain

Cette étude s'inscrit dans un positionnement épistémologique interprétativiste modéré (Girod-Séville & Perret, 1999) et adopte un design exploratoire à méthodes mixtes (Creswell &

Creswell, 2018). Ce positionnement est cohérent avec l'objet de recherche : les risques logistiques et les pratiques Leagile sont des phénomènes socialement construits, dont la signification ne peut être pleinement appréhendée qu'à travers les perceptions et les expériences des acteurs qui les vivent au quotidien. L'objectif n'est donc pas de mesurer des relations causales universelles, mais de comprendre comment une configuration organisationnelle spécifique produit des effets de résilience dans un contexte particulier (Girod-Séville & Perret, 1999 ; Yin, 2014). Le recours à des méthodes mixtes répond à la nécessité de croiser deux types de données complémentaires : des données déclaratives sur les perceptions et les pratiques, et des données observationnelles sur les comportements effectifs en situation réelle.

L'étude a été conduite au sein d'une organisation industrielle marocaine dont l'activité implique la gestion de flux logistiques continus, à fort volume et à caractère critique. Le choix de ce terrain répond à trois critères de pertinence : la diversité et la récurrence des risques logistiques auxquels l'organisation est exposée, la coexistence de pratiques Lean formalisées et de pratiques agiles développées de manière informelle par les équipes opérationnelles, et l'accessibilité négociée avec la direction dans le cadre d'engagements éthiques stricts. Par souci de confidentialité et conformément aux engagements pris avec les répondants, l'identité de l'organisation n'est pas divulguée.

3.2 Instruments de recueil et analyse des données

Le recueil repose sur deux instruments administrés de manière concomitante, dont la combinaison vise à renforcer la validité interne par triangulation (Yin, 2014).

Le questionnaire structuré a été administré à 41 collaborateurs sélectionnés selon un échantillonnage raisonné couvrant trois niveaux hiérarchiques : des responsables de service (cadres en charge de la planification et de la supervision), des contrôleurs et superviseurs intermédiaires, et des agents opérationnels de terrain. Ce choix d'échantillonnage raisonné multi-niveaux, conformément aux recommandations de Miles, Huberman et Saldaña (2014) pour les études exploratoires en contexte organisationnel, visait à croiser les perceptions du management stratégique, de l'encadrement intermédiaire et des opérateurs sur les mêmes risques et les mêmes pratiques permettant ainsi d'identifier d'éventuels écarts de perception entre niveaux hiérarchiques. Le questionnaire comportait des items organisés en trois blocs thématiques : (1) la perception et la fréquence des risques logistiques rencontrés, évaluées sur une échelle de Likert à cinq points ; (2) la connaissance et l'utilisation des pratiques Lean et agiles, mesurées sur une échelle de fréquence ; et (3) l'efficacité perçue de ces pratiques face

aux perturbations, évaluée sur une échelle d'accord. Cet ancrage des items dans les typologies établies par Lavastre et al. (2012) et Chopra et Sodhi (2004) garantit la validité de construit du questionnaire.

3.3 Validité du dispositif et limites

La rigueur d'une étude exploratoire qualitative se mesure moins à sa représentativité statistique qu'à la qualité de son dispositif de validation interne et à la transparence de ses limites (Miles, Huberman & Saldaña, 2014). Trois dimensions de validité sont examinées ici.

La validité interne repose sur la triangulation systématique des données questionnaire et observationnelles : chaque catégorie de risque identifiée par questionnaire a été confrontée aux pratiques observées directement sur le terrain, permettant de distinguer ce que les acteurs déclarent faire de ce qu'ils font effectivement. Cette triangulation a également permis de détecter des pratiques hybrides non formalisées, notamment les réunions journalières à double fonction Lean/Agile qui n'auraient pas émergé d'un questionnaire seul. Le biais de désirabilité sociale, inhérent aux auto-déclarations, a été partiellement contrôlé par l'anonymat garanti aux répondants et par la confrontation systématique avec les observations directes.

La validité de construit est assurée par l'ancrage des items du questionnaire dans les typologies théoriques établies (Lavastre et al., 2012 ; Chopra & Sodhi, 2004) et par la mise en correspondance des catégories empiriques avec les concepts issus de la revue de littérature. Les propositions de recherche P1 et P2 formulées en section 2 ont guidé la lecture des données de manière à éviter une dérive purement inductive, insuffisamment ancrée dans la littérature.

La validité externe est, en revanche, structurellement limitée par la nature mono-site de l'étude et par la taille de l'échantillon ($n = 41$), qui ne permettent pas de généralisations statistiques. Ces limites sont constitutives du design exploratoire retenu, dont l'objectif n'est pas de tester des relations causales mais de générer des propositions théoriques testables et de produire une compréhension contextualisée du phénomène étudié (Girod-Séville & Perret, 1999 ; Yin, 2014). La généralisation visée est donc de nature analytique (transfert du cadre intégrateur proposé à d'autres contextes industriels) et non statistique. Ces limites ouvrent des pistes de recherche confirmatoires discutées en section 6.

4. Résultats et analyses

4.1 Cartographie des risques logistiques identifiés

L'analyse croisée des données questionnaire et observationnelles a permis d'identifier cinq catégories de risques logistiques récurrents, recoupant les typologies de Lavastre et al. (2012) tout en présentant des spécificités propres au contexte industriel marocain. Ces cinq catégories ne présentent pas la même importance perçue : leur hiérarchisation selon la fréquence et l'intensité constitue en elle-même un résultat analytique significatif, dans la mesure où elle conditionne la nature et l'intensité des réponses organisationnelles mobilisées.

Les risques opérationnels ressortent comme la catégorie la plus importante, tant en fréquence déclarée qu'en intensité perçue. Les responsables insistent unanimement sur leur caractère cascasant : une panne non traitée rapidement perturbe l'ensemble de la chaîne par effet de propagation. Les risques de coordination inter-services constituent la catégorie la plus complexe, émergeant non d'un incident isolé mais d'une désynchronisation structurelle entre planification, transport et maintenance, perçue différemment selon le niveau hiérarchique : déficit d'information pour les responsables, contraintes de délai et de ressources pour les agents de terrain. Les risques de transport, liés aux stocks et humains et HSE, bien que d'intensité variable, sont identifiés par l'ensemble des répondants avec des nuances selon leur position hiérarchique. Le Tableau 1 synthétise la hiérarchisation de ces cinq catégories.

Tableau 1 : Hiérarchisation des risques logistiques selon leur fréquence et leur intensité perçues

Catégorie de risque	Fréquence perçue	Intensité perçue	caractère cascasant	Niveau de formalisation des réponses
Risques opérationnels	Très élevée	Très élevée	Oui	Élevé (TPM, ARPT)
Risques de coordination	Très élevée	Très élevée	Oui	Modéré (réunion, tableaux de bord)
Risques humains et HSE	Élevée	Modérée	Partiel	Élevé (formations, audits)

Risques liés aux stocks	Modérée	Élevée	Non	Modéré (suivi indicateurs)
Risques de transport	Modérée	Élevée	Non	Modéré (inspections, standards)

Source : Autrices, d'après les données du questionnaire et les observations directes

4.2 Configuration Leagile et résilience : une articulation synergique

L'analyse des pratiques déployées révèle une complémentarité systémique entre les deux registres, dont l'articulation relève d'une configuration organisationnelle émergente progressivement construite par les équipes au fil des perturbations, rejoignant les conclusions de Tortorella et al. (2020) sur le rôle central de l'apprentissage organisationnel.

Les pratiques Lean (TPM, ARPT, standards HSE, réunions journalières de planification, suivi quotidien des indicateurs) opèrent en amont des perturbations dans une logique de prévention et de standardisation, réduisant la fréquence et la sévérité des risques prévisibles. Cette logique préventive constitue ce que Shah et Ward (2007) conceptualisent comme une réduction structurelle de la variabilité opérationnelle. Les pratiques agiles (mobilisation rapide d'équipes de maintenance, wagons de réserve, reconfiguration immédiate des rotations, autonomie et décision décentralisée) entrent en jeu lors des perturbations pour absorber les chocs imprévus et accélérer le rétablissement, conformément à la définition de la résilience logistique de Ponomarov et Holcomb (2009). Le Tableau 2 documente cette configuration.

Tableau 2 : Configuration Leagile et réduction des risques logistiques dans l'organisation étudiée

Catégories de risques	Illustrations terrain	Pratiques Lean mobilisées	Pratiques Agiles mobilisées	Effets sur la résilience
Risques opérationnels	Pannes d'équipements, incidents, anomalies répétées	TPM, ARPT*, maintenance préventive planifiée	Mobilisation rapide d'équipes, reconfiguration des flux	Réduction des arrêts, continuité des opérations

Risques de transport	de	Indisponibilité de wagons, perturbations ferroviaires	de	Inspections régulières, standards HSE formalisés	Wagons de réserve, renfort urgent, ajustement rotations	Continuité des flux de transport
Risques de coordination	de	Désynchronisation inter-services, ajustements tardifs		Réunions journalières, tableaux de bord partagés	Flexibilité des rotations, reconfiguration des plannings	Fluidité des échanges, réduction des délais
Risques liés aux stocks	liés	Ruptures ou surstocks, décalages prévisions/réalité		Suivi quotidien des niveaux, indicateurs de performance	Ajustements rapides, recours à fournisseurs alternatifs	Équilibre offre-demande, limitation des ruptures
Risques humains HSE	et	Erreurs opérateur, incidents terrain, non-respects procédures		Formations standardisées, procédures HSE, audits internes	Autonomie opérationnelle, décision décentralisée	Réduction erreurs humaines, culture sécurité renforcée
* ARPT : Analyse des Risques liés aux Postes du Travail— ensemble de fiches différenciées par poste de travail, recensant les risques susceptibles d'être rencontrés et les actions préventives et correctives associées.						

Source : Autrices, d'après les données du questionnaire et les observations directes.

Au-delà de cette complémentarité, les données révèlent un résultat analytique plus original : certaines pratiques remplissent simultanément une fonction Lean et une fonction agile. Les réunions journalières de planification en constituent l'exemple le plus parlant, elles standardisent la coordination inter-services (Lean) tout en permettant un ajustement rapide aux imprévus (agilité) ; de même, les tableaux de bord partagés assurent le suivi des indicateurs (Lean) et la diffusion en temps réel des informations critiques (agilité). Nous proposons de conceptualiser ces pratiques comme des pratiques hybrides ambidextres, notion absente de la littérature existante sur le Leagile, qui suggère que la frontière entre les deux paradigmes est

dans la réalité organisationnelle plus poreuse que ne le laisse supposer le modèle théorique fondateur (Mason-Jones et al., 2000 ; Towill & Christopher, 2002).

Ces résultats apportent un soutien initial, quoique non conclusif, aux deux propositions formulées en section 2. Concernant P1, les équipes dont les pratiques Lean sont les plus formalisées mobilisent les réponses agiles les plus rapides et les mieux coordonnées; la stabilisation Lean semble créer les conditions qui rendent l'agilité opérationnellement possible et efficace. Concernant P2, les équipes combinant spontanément standardisation et flexibilité présentent des capacités de récupération notablement supérieures. Ces observations fournissent une base empirique cohérente pour justifier le test confirmatoire de P1 et P2 sur des échantillons plus larges.

La Figure 2 synthétise ces résultats dans un cadre intégrateur original, modélisant le processus cyclique par lequel la stratégie Leagile produit de la résilience logistique : l'identification des risques déclenche simultanément une réponse Lean et une réponse agile ; leur synergie produit une résilience renforcée ; celle-ci alimente en retour un apprentissage organisationnel continu qui améliore progressivement la configuration. Ce processus dynamique, dont l'efficacité se renforce à chaque cycle perturbation-réponse-apprentissage, converge avec les travaux de Chowdhury et Quaddus (2017) sur les capacités dynamiques comme fondements de la résilience logistique.

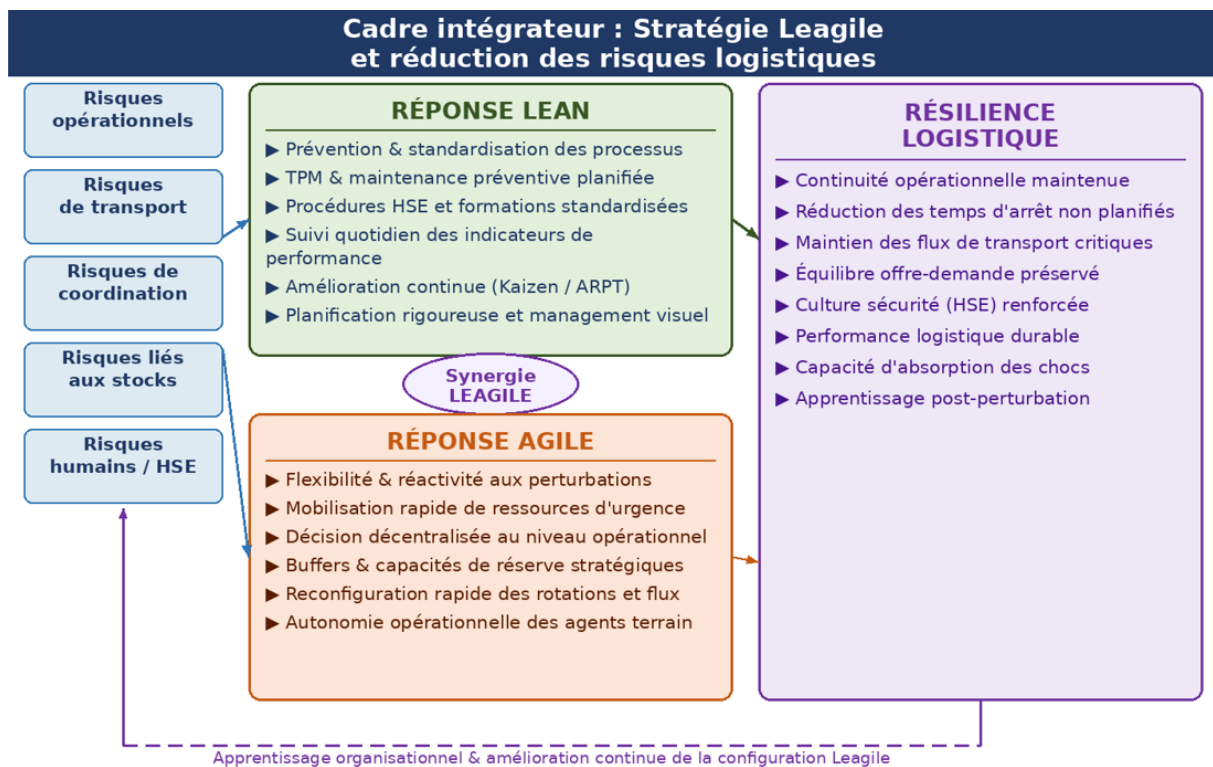


Figure 2 : Cadre intégrateur : stratégie Leagile et réduction des risques logistiques

Source : Élaboration des autrices, d'après les données du terrain et la revue de littérature.

5. Discussion et implications

5.1 Contributions théoriques : Mise en perspective avec la littérature

Les résultats appellent une mise en perspective théorique autour de trois contributions distinctes.

La première est l'extension du modèle Leagile à l'ensemble des dimensions opérationnelles de la logistique. Les travaux fondateurs de Mason-Jones et al. (2000) ont conceptualisé le Leagile essentiellement autour de la gestion des stocks et du point de découplage. Nos résultats montrent que cette conceptualisation sous-estime la portée réelle du Leagile : dans l'organisation étudiée, la configuration opère également sur la coordination inter-services, la gestion des ressources humaines et la culture sécurité. Cette extension prolonge les travaux de Krishnamurthy et Yauch (2007) et converge avec les appels de Tortorella et al. (2020) à considérer l'hybridation Lean/Agile comme une compétence organisationnelle transversale.

La deuxième est la conceptualisation des pratiques hybrides ambidextres. En documentant des pratiques remplissant simultanément une fonction Lean et une fonction agile, notre étude suggère que la réalité organisationnelle est plus complexe que ne le laisse supposer le modèle théorique fondateur. Ce résultat entre en dialogue avec les travaux sur l'ambidextrie organisationnelle (Gibson & Birkinshaw, 2004), qui montrent que les organisations les plus résilientes combinent simultanément standardisation et flexibilité, deux polarités dont le Lean et l'agilité constituent des expressions opérationnelles dans le champ logistique.

La troisième est le rôle de l'apprentissage organisationnel comme mécanisme de consolidation de la configuration Leagile. La configuration observée n'est pas le fruit d'une planification délibérée mais d'un processus émergent (Weick, 2000), progressivement construit par les équipes au fil des perturbations. Cette observation enrichit la thèse de Mason-Jones et al. (2000) en montrant que la valeur du Leagile réside non seulement dans l'architecture de la chaîne logistique, mais dans la capacité organisationnelle à la faire évoluer par apprentissage continu, en dialogue avec les travaux sur les capacités dynamiques (Teece et al., 2016 ; Chowdhury & Quaddus, 2017). Ces trois contributions apportent un soutien initial à P1 et P2, et plaident pour leur test confirmatoire par modélisation par équations structurelles sur des échantillons plurisectoriels (Tortorella et al., 2020 ; Brusset & Teller, 2017).

5.2 Ancrage dans la conduite du changement et implications managériales

Au-delà de ses apports théoriques, cette étude produit des enseignements pratiques directement mobilisables par les responsables logistiques opérant dans des environnements similaires. L'adoption d'une configuration Leagile constitue en elle-même une démarche de conduite du changement organisationnel : elle implique une transformation des représentations, dépasser

l'opposition entre Lean et agilité pour les concevoir comme complémentaires, une reconfiguration des pratiques opérationnelles et une évolution culturelle vers plus d'autonomie et de flexibilité (Soparnot, 2004). Sur le terrain étudié, ce changement a émergé progressivement par apprentissage collectif plutôt que par une démarche planifiée descendante (Weick, 2000 ; Kotter, 1996), suggérant que la transition vers le Leagile peut être facilitée par des dynamiques bottom-up, à condition que le management crée les conditions favorables à l'autonomie et à l'expérimentation.

Trois implications pratiques se dégagent. La première concerne la complémentarité des investissements Lean et agiles : nos résultats montrent que ces deux types d'investissements ne sont pas substituables mais synergiques. Une infrastructure Lean solide (procédures standardisées, maintenance préventive rigoureuse, indicateurs de suivi fiables) crée les conditions d'une agilité plus efficace en réduisant la variabilité de fond et en libérant des capacités pour la gestion des imprévus. La deuxième implication concerne l'autonomie opérationnelle des agents de terrain : les pratiques agiles les plus efficaces (reconfiguration rapide des rotations, mobilisation d'équipes de renfort, ajustements décisionnels en temps réel) reposent sur une décentralisation effective des prises de décision. Nos résultats suggèrent que cette autonomie, encadrée par des standards Lean bien intégrés, constitue un levier décisif de résilience que les organisations gagneraient à développer plutôt qu'à contraindre. La troisième implication concerne la valorisation des pratiques hybrides ambidextres : les réunions journalières de planification et les tableaux de bord partagés constituent des dispositifs organisationnels précieux que les organisations industrielles gagneraient à identifier systématiquement, à documenter et à diffuser, plutôt que de les laisser à l'état de routines informelles non reconnues.

6. Conclusion, limites et perspectives de recherche

Ce chapitre a examiné empiriquement comment la stratégie Leagile contribue à la réduction des risques logistiques dans un environnement industriel marocain. En mobilisant un dispositif mixte auprès de 41 collaborateurs répartis sur trois niveaux hiérarchiques, il a permis d'identifier cinq catégories de risques récurrents et de documenter leur articulation avec les pratiques Lean et agiles déployées. Les résultats révèlent une configuration Leagile cohérente et synergique, dont l'efficacité repose sur la complémentarité structurelle des deux paradigmes, sur l'existence de pratiques hybrides ambidextres et sur un processus d'apprentissage organisationnel continu.

Les contributions de ce travail s'articulent à trois niveaux. Au niveau conceptuel, il enrichit la théorisation du Leagile en démontrant que sa contribution à la résilience dépasse la gestion des stocks pour s'étendre à la coordination inter-services, aux ressources humaines et à la culture sécurité. La notion de pratiques hybrides ambidextres, absente de la littérature existante, constitue un apport original invitant à repenser la frontière théorique entre Lean et agilité comme une zone de porosité productive. Au niveau empirique, il documente la configuration Leagile dans un contexte industriel marocain peu représenté dans la littérature internationale, montrant que les spécificités de ce contexte modèlent les formes concrètes d'expression du Leagile sans en compromettre l'efficacité. Les propositions P1 et P2 reçoivent un soutien empirique initial cohérent, qui justifie leur test confirmatoire sur des échantillons plus larges. Au niveau méthodologique, le cadre intégrateur proposé (Figure 2) formalise le processus cyclique Leagile — identification des risques, réponses Lean et agiles, résilience renforcée, apprentissage organisationnel — et offre une base opérationnalisable pour des recherches futures.

Les principales limites tiennent au caractère mono-site de l'étude, à la taille réduite de l'échantillon ($n = 41$) et à l'absence d'indicateurs quantitatifs objectifs de performance logistique. Ces limites, constitutives du design exploratoire retenu, ouvrent trois perspectives de recherche concrètes : la réplication sur des échantillons plurisectoriels comparatifs entre contextes marocain, africain et européen ; le développement d'une échelle de mesure de la maturité Leagile intégrant une dimension spécifique aux pratiques hybrides ambidextres ; et le test confirmatoire de P1 et P2 par modélisation par équations structurelles (SEM), en réponse aux appels de Tortorella et al. (2020), Chowdhury et Quaddus (2017) et Brusset et Teller (2017).

Références bibliographiques

- Brusset, X., & Teller, C. (2017). Supply chain capabilities, risks, and resilience. *International Journal of Production Economics*, 184, 59-68.
- Chopra, S. and Sodhi, M.S. (2004) Managing risk to avoid supply-chain breakdown. *MIT Sloan Management Review*, 46 (1), 53-61.
- Chowdhury, M. M. H., & Quaddus, M. (2017). Supply Chain Resilience: Conceptualization and Scale Development Using Dynamic Capability Theory. *International Journal of Production Economics*, 188, 185-204.
- Christopher, M. (2000) The Agile Supply Chain: Competing in Volatile Markets. *Industrial Marketing Management*, 29, 37-44.

- Christopher, M. and Towill, D. (2001) An Integrated Model for the Design of Agile Supply Chains. *International Journal of Physical Distribution & Logistics Management*, 31, 235-246.
- Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative and mixed methods approaches* (5e éd.). SAGE Publications.
- Gibson, C. B., & Birkinshaw, J. (2004). The antecedents, consequences, and mediating role of organizational ambidexterity. *Academy of Management Journal*, 47(2), 209-226.
- Girod-Séville, M., & Perret, V. (1999). Fondements épistémologiques de la recherche. Dans R.-A. Thiétart (dir.), *Méthodes de recherche en management* (pp. 13-33). Dunod.
- Gunasekaran, A. (1999). Agile manufacturing: A framework for research and development. *International Journal of Production Economics*, 62(1-2), 87-105.
- Ivanov, D. (2022). Viable supply chain model: Integrating agility, resilience and sustainability perspectives — lessons from and thinking beyond the COVID-19 pandemic. *Annals of Operations Research*, 319, 1411-1431.
- Ivanov, D., & Dolgui, A. (2021). A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0. *Production Planning & Control*, 32(9), 775-788.
- Jüttner, U., Peck, H., & Christopher, M. (2003). Supply chain risk management: Outlining an agenda for future research. *International Journal of Logistics: Research and Applications*, 6(4), 197-210.
- Kleindorfer, P. R., & Saad, G. H. (2005). Managing disruption risks in supply chains. *Production and Operations Management*, 14(1), 53-68.
- Kotter, J. P. (1996). *Leading change*. Harvard Business School Press.
- Krishnamurthy, R., & Yauch, C. A. (2007). Leagile manufacturing: A proposed corporate infrastructure. *International Journal of Operations & Production Management*, 27(6), 588-604.
- Lavastre, O., Gunasekaran, A., & Spalanzani, A. (2012). Supply chain risk management in French companies. *Decision Support Systems*, 52(4), 828-838.
- Liker, J. K. (2004). *The Toyota way: 14 management principles from the world's greatest manufacturer*. McGraw-Hill.

- Mason-Jones, R., Naylor, B., & Towill, D. R. (2000). Lean, agile or leagile? Matching your supply chain to the marketplace. *International Journal of Production Research*, 38(17), 4061-4070.
- Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook* (3e éd.). SAGE Publications.
- Naylor, J. B., Naim, M. M., & Berry, D. (1999). Leagility: Integrating the lean and agile manufacturing paradigms in the total supply chain. *International Journal of Production Economics*, 62(1-2), 107-118.
- Netland, T. H., & Powell, D. J. (Éds.). (2017). *The Routledge companion to lean management*. Routledge.
- Ponomarov, S. Y., & Holcomb, M. C. (2009). Understanding the concept of supply chain resilience. *International Journal of Logistics Management*, 20(1), 124-143.
- Queiroz, M. M., Ivanov, D., Dolgui, A., & Fosso Wamba, S. (2020). Impacts of epidemic outbreaks on supply chains: Mapping a research agenda amid the COVID-19 pandemic through a structured literature review. *Annals of Operations Research*, 319(1), 1159-1196.
- Rossini, M., Costa, F., Tortorella, G. L., & Portioli-Staudacher, A. (2019). The interrelation between Industry 4.0 and lean production: An empirical study on European manufacturers. *International Journal of Advanced Manufacturing Technology*, 102(9-12), 3963-3976.
- Sarkis, J., Cohen, M. J., Dewick, P., & Schröder, P. (2020). A brave new world: Lessons from the COVID-19 pandemic for transitioning to sustainable supply and production. *Resources, Conservation and Recycling*, 159, 104894.
- Shah, R., & Ward, P. T. (2007). Defining and developing measures of lean production. *Journal of Operations Management*, 25(4), 785-805.
- Soparnot, R. (2004). L'évaluation des modèles de gestion du changement organisationnel : de la capacité de gestion du changement à la gestion des capacités de changement. *Gestion*, 29(4), 31-42.
- Tang, C. S. (2006). Perspectives in supply chain risk management. *International Journal of Production Economics*, 103(2), 451-488.
- Teece, D., Peteraf, M., & Leih, S. (2016). Dynamic capabilities and organizational agility. *California Management Review*, 58(4), 13-35.

- Tortorella, G. L., Vergara, A. M. C., Garza-Reyes, J. A., & Sawhney, R. (2020). Organizational learning paths based upon Industry 4.0 adoption: An empirical study with Brazilian manufacturers. *International Journal of Production Economics*, 219, 284-294.
- Towill, D. R., & Christopher, M. (2002). The supply chain strategy conundrum: To be lean or agile or to be lean and agile? *International Journal of Logistics: Research and Applications*, 5(3), 299-309.
- Weick, K. E. (2000). Emergent change as a universal in organizations. Dans M. Beer & N. Nohria (Éds.), *Breaking the code of change* (pp. 223-241). Harvard Business School Press.
- Womack, J. P., & Jones, D. T. (1996). *Lean thinking: Banish waste and create wealth in your corporation*. Simon & Schuster.
- Yin, R. K. (2014). *Case study research: Design and methods* (5e éd.). SAGE Publications.
- Zsidisin, G. A. (2003). A grounded definition of supply risk. *Journal of Purchasing and Supply Management*, 9(5-6), 217-224.

CHAPITRE 7: *Dispositifs de contrôle de gestion et résilience organisationnelle : quelle contribution à la maîtrise des risques dans les établissements universitaires publics ?*

TOUZANI Fatima Zahra

Doctorante au Laboratoire Business Intelligence, Gouvernance des Organisations, Finance et Politiques Économiques-FSJES Ain Chock, Université Hassan II de Casablanca-
fatizahratouzani@gmail.com

Les établissements universitaires publics sont aujourd'hui confrontés à une pression simultanée sur leurs missions, leurs ressources et leurs modes de fonctionnement : massification des effectifs, exigences d'accréditation, contraintes budgétaires, digitalisation des processus administratifs et pédagogiques, et attentes accrues en matière de transparence. Dans un tel contexte, la continuité du service ne dépend plus uniquement de la conformité des procédures, mais de la capacité institutionnelle à anticiper les perturbations, à absorber leurs effets et à ajuster les décisions. Cette capacité renvoie à la résilience organisationnelle, entendue comme un ensemble de compétences collectives permettant l'anticipation, la réponse et l'apprentissage face aux tensions (Duchek, 2020).

La littérature sur la gestion des risques insiste sur l'importance d'une démarche structurée, continue et reliée aux objectifs, articulant identification, évaluation, traitement et suivi des risques (ISO, 2018; COSO, 2017). Toutefois, dans de nombreuses organisations publiques, les risques restent traités de manière partielle ou implicite, tandis que les instruments de pilotage produisent parfois davantage de conformité documentaire que de capacité d'action. Dans les universités publiques, les dispositifs de contrôle de gestion constituent dès lors un point d'entrée stratégique : selon leur conception et leur appropriation, ils peuvent rester cantonnés au suivi budgétaire ou devenir des mécanismes de coordination, d'arbitrage et d'apprentissage organisationnel. Ainsi, la question principale de cette recherche peut être énoncée comme suit : *dans quelle mesure, et à quelles conditions, les dispositifs de contrôle de gestion contribuent-ils à la maîtrise des risques et au renforcement de la résilience organisationnelle dans les établissements universitaires publics?*

L'objectif de l'article est de caractériser les configurations d'usage du contrôle de gestion face aux risques et d'identifier les conditions organisationnelles qui permettent de dépasser une logique principalement conformiste. Ainsi, deux hypothèses guident cette analyse. La première postule que le contrôle de gestion, lorsqu'il articule objectifs, indicateurs, tableaux de bord, routines de suivi et arbitrages formalisés, facilite l'intégration du risque dans la décision et renforce des capacités d'anticipation, de coping et d'apprentissage. La seconde suggère que cette contribution demeure conditionnelle : elle dépend du portage de la gouvernance, de la qualité des données, de la maturité des systèmes d'information, des compétences de pilotage et d'une culture de transparence.

Le développement s'organise en cinq temps. La première partie précise le cadre théorique, le périmètre des risques retenus et le modèle d'analyse. La deuxième présente la méthodologie qualitative adoptée. La troisième expose les résultats sous forme de configurations d'usage du contrôle de gestion. La quatrième discute les hypothèses et les apports de l'étude au regard de la littérature. La conclusion synthétise les implications, les limites et les pistes de recherche.

1. Cadre théorique, périmètre du risque et modèle d'analyse

1.1. Risque universitaire et logique ERM

Dans le champ universitaire, la notion de risque est souvent mobilisée de manière large. Pour en faire un objet pilotable, l'article retient une définition orientée objectifs : un risque

correspond à l'effet de l'incertitude sur la réalisation des missions de continuité, de qualité et de soutenabilité (ISO, 2018). L'étude ne cherche donc pas à couvrir tous les risques possibles, mais à examiner ceux qui peuvent être rendus visibles par les instruments de pilotage, discutés dans les routines de gestion et traités par des arbitrages.

Quatre familles de risques sont privilégiées, car elles apparaissent de manière récurrente dans le matériau empirique et se prêtent à une observation à travers les dispositifs de contrôle : les risques informationnels liés à la qualité et à la cohérence des données ; les risques financiers liés aux retards de paiement, aux rigidités budgétaires et aux prestataires critiques ; les risques numériques relatifs à l'indisponibilité des plateformes et à la cybersécurité ; enfin, les risques de capacité et de continuité de service liés à la massification, à la charge d'enseignement et à la pression sur les locaux. Ce périmètre s'inscrit dans une logique ERM, selon laquelle l'enjeu n'est pas de juxtaposer des catégories de risques, mais de relier les incertitudes aux objectifs et aux décisions (COSO, 2017).

1.2. Contrôle de gestion : d'un outil de suivi à un système de pilotage

L'article adopte une conception systémique du contrôle de gestion. Celui-ci ne se réduit pas à un budget, à un reporting ou à quelques indicateurs, mais forme un package combinant planification, contrôle cybernétique, dispositifs administratifs, mécanismes culturels et routines d'échange (Malmi & Brown, 2008). Dans les universités publiques, cette perspective est particulièrement utile, car l'organisation est plurielle : elle combine enseignement, recherche, services à la société, autonomie relative des établissements et forte dépendance aux règles de conformité.

La distinction proposée par Simons (1995) entre usage diagnostique et usage interactif des systèmes de contrôle éclaire directement l'analyse. Un usage diagnostique permet de constater les écarts, de suivre l'exécution et de rendre compte. Un usage interactif, en revanche, transforme les données en support de discussion sur les incertitudes, les priorités et les arbitrages. Dans un environnement universitaire marqué par la digitalisation, la pression budgétaire et l'hétérogénéité des données, c'est précisément cette dimension interactive qui peut faire du contrôle de gestion un levier de maîtrise des risques.

1.3. Résilience organisationnelle : anticipation, coping et adaptation

La résilience organisationnelle est retenue comme une capacité dynamique et non comme une simple résistance. La grille de Duchek (2020) permet de la saisir autour de trois moments : l'anticipation, qui renvoie à la détection des signaux faibles et à la préparation ; le coping, qui désigne la réponse en situation perturbée et la continuité sous tension ; l'adaptation, qui correspond à l'apprentissage et à la transformation des routines après l'événement. Cette conception présente un intérêt méthodologique, car elle rend la résilience observable dans les données empiriques : existence de seuils d'alerte, revues de performance, arbitrages en situation de contrainte, retours d'expérience et révision des procédures.

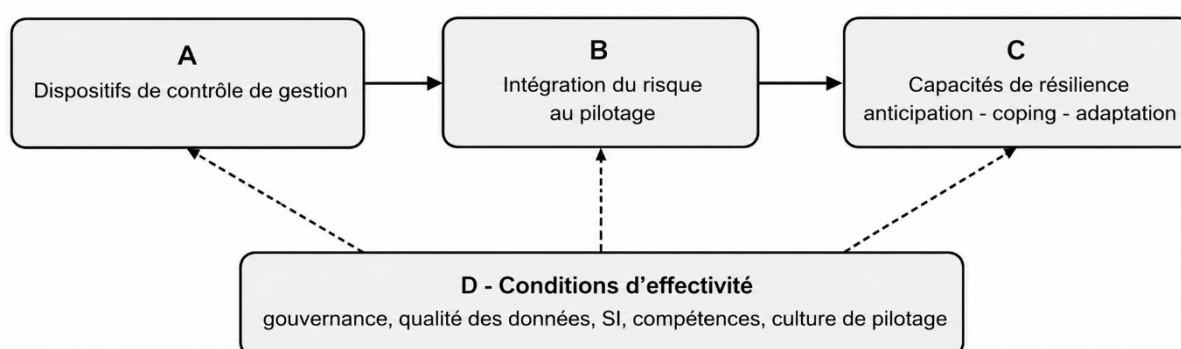
Dans une université publique, l'anticipation peut porter sur les tensions d'inscription, les besoins en locaux, les vulnérabilités des plateformes ou les délais de paiement. Le coping se manifeste lorsque l'établissement doit préserver des processus vitaux comme les examens, la

paie, les achats ou la continuité pédagogique. L'adaptation apparaît lorsque l'incident conduit à formaliser un apprentissage durable : fiabilisation des données, renforcement du contrôle interne, sécurisation des systèmes d'information ou révision des mécanismes d'arbitrage.

1.4.Modèle d'analyse

Le modèle d'analyse repose sur une idée centrale : le contrôle de gestion contribue à la maîtrise des risques et à la résilience lorsqu'il transforme l'incertitude en information discutée, puis en arbitrages suivis. Il articule quatre blocs : les dispositifs de contrôle de gestion (A), l'intégration du risque au pilotage (B), les capacités de résilience (C) et les conditions d'effectivité (D). Ces dernières — gouvernance, qualité des données, maturité des systèmes d'information, compétences et culture de pilotage — conditionnent le passage d'un contrôle rituel à un contrôle réellement opérant.

Figure 3: Modèle d'analyse reliant contrôle de gestion, maîtrise des risques et résilience



Source : Élaboration de l'auteure à partir de Malmi et Brown (2008), Simons (1995), COSO (2017), ISO (2018) et Duchek (2020).

2. Méthodologie et dispositif d'enquête

2.1.Choix du design et logique de terrain

Pour comprendre ce que font réellement les dispositifs de contrôle de gestion dans les universités publiques, l'étude adopte un design qualitatif fondé sur des cas multiples. L'objectif n'est pas de mesurer statistiquement un effet isolé, mais de reconstituer des mécanismes : comment une contrainte devient un arbitrage, comment un indicateur déclenche ou non une discussion, et comment une alerte se transforme ou non en action. Cette approche permet une généralisation analytique, fondée sur la comparaison de configurations organisationnelles (Eisenhardt, 1989; Yin, 2018).

Le terrain couvre dix établissements relevant de trois universités marocaines : l'Université Hassan II de Casablanca, l'Université Hassan I de Settat et l'Université Chouaib Doukkali d'El Jadida. Ce choix vise une variation utile : les établissements sont comparables par leur statut

public et leurs contraintes institutionnelles, mais suffisamment différenciés pour observer des manières distinctes de piloter, de rendre compte et d'intégrer la dimension risque dans les routines de gestion.

2.2. Collecte des données et construction du corpus

La collecte des données a été menée au cours du deuxième semestre 2025. Elle repose principalement sur quinze entretiens semi-directifs réalisés auprès de responsables occupant des fonctions liées à la gouvernance, à la planification, aux affaires administratives et financières, à la qualité et aux systèmes d'information. Les entretiens ont été réalisés en présentiel et à distance par téléphone. Leur durée varie entre 35 et 45 minutes, avec une moyenne d'environ 40 minutes. Les entretiens ont été intégralement retranscrits puis traités avec le logiciel NVivo, afin d'assurer une organisation systématique du matériau empirique.

Le guide d'entretien a été conçu pour maintenir une trame comparable entre établissements tout en laissant émerger les routines informelles, les irritants, les contradictions et les arbitrages réels. Les entretiens ont été complétés par une analyse documentaire ciblée : tableaux de bord, documents de programmation, rapports internes, procédures qualité, référentiels d'évaluation, notes de gestion et documents relatifs à la transformation numérique lorsque ceux-ci étaient disponibles. Cette triangulation permet de confronter les discours aux instruments effectivement produits et de repérer les écarts entre l'outil tel qu'il existe et l'outil tel qu'il est utilisé (Yin, 2018).

2.3. Stratégie d'analyse et garanties de rigueur

L'analyse a été conduite selon une logique thématique appuyée par NVivo. Elle s'est déroulée en plusieurs étapes : familiarisation avec le corpus, codage initial, regroupement des codes, stabilisation des thèmes et confrontation des résultats au modèle d'analyse. Cette démarche s'inspire des principes de l'analyse thématique proposés par Braun et Clarke (2006), tout en mobilisant des matrices de comparaison intra-cas et inter-cas afin de relier instruments, acteurs, routines et effets perçus sur la maîtrise des risques (Miles et al., 2014).

La rigueur de la démarche repose sur trois précautions principales : la diversité des profils interrogés, la triangulation entre entretiens et documents, et la transparence du chemin analytique reliant verbatim, thèmes et configurations. La transférabilité est recherchée par une description suffisamment précise du contexte, de la collecte et de l'analyse, afin que le lecteur puisse apprécier les conditions dans lesquelles les résultats pourraient être mobilisés dans d'autres environnements universitaires (Lincoln & Guba, 1985).

3. Résultats : usages du contrôle de gestion et contribution à la maîtrise des risques

3.1. Résultats transversaux

Les entretiens mettent d'abord en évidence une tension entre un contrôle de gestion mobilisé comme obligation de reporting et un contrôle de gestion utilisé comme outil de pilotage. Dans plusieurs établissements, l'énergie des acteurs est absorbée par la production de tableaux et la remontée d'informations, sans retour structuré ni apprentissage. Un responsable administratif et financier résume cette expérience en évoquant un reporting essentiellement descendant :

« On passe un temps considérable à remplir des tableaux Excel pour l'université ou le ministère. Une fois envoyés, on reçoit rarement un retour. On a l'impression de piloter pour la forme, pas pour anticiper les problèmes de trésorerie ou de ressources. »

Un second résultat transversal concerne le risque informationnel. La qualité, la cohérence et la circulation des données conditionnent directement la capacité d'anticipation. Lorsque les chiffres divergent selon les services ou les systèmes, le pilotage devient fragile. Un responsable de la planification l'exprime clairement :

« Le plus gros risque, c'est l'aveuglement. J'ai trois chiffres différents pour le nombre d'étudiants inscrits selon que je demande à la scolarité, au service informatique ou aux départements. Comment anticiper les besoins en locaux avec ça ? »

Enfin, la dimension risque apparaît souvent vécue mais peu formalisée. Les acteurs savent identifier ce qui fragilise l'établissement, mais cette conscience ne se traduit pas toujours par des dispositifs stables : cartographie vivante, seuils d'alerte, plan de traitement ou retour d'expérience. Un responsable qualité décrit ce décalage :

« Si vous demandez aux chefs de service où est leur cartographie des risques, ils vous montrent un document ancien. Mais si vous leur demandez ce qui les empêche de dormir, ils citent immédiatement la panne du serveur pendant les examens ou le départ d'un technicien clé. »

3.2. Trois configurations d'usage du contrôle de gestion face au risque

Les résultats peuvent être organisés autour de trois configurations dominantes. Elles ne figent pas chaque établissement dans une catégorie unique, mais permettent de rendre intelligibles des combinaisons d'outils, de routines et de rapports au risque.

Dans la première configuration, le contrôle de gestion est dominé par une logique de conformité. Le pilotage est assimilé à la production de preuves, à la sécurisation des dossiers et à la réduction des écarts formels. Cette logique peut créer une fausse sécurité : la présence de visas et de contrôles a priori est interprétée comme une maîtrise suffisante, alors que les vulnérabilités réelles se déplacent vers la fiabilité des prestataires, la continuité de service ou la dépendance à des ressources critiques. Un cadre financier l'illustre ainsi :

« On a tellement de procédures de contrôle a priori qu'on finit par croire que le risque est maîtrisé. On vérifie la facture, mais on ne voit pas toujours que le prestataire ne pourra pas livrer le matériel attendu. »

Dans la deuxième configuration, le contrôle de gestion est orienté vers la performance, mais demeure segmenté. Les indicateurs existent et permettent un suivi plus régulier de l'activité ; toutefois, ils restent souvent rattachés à des services distincts, sans espace transversal d'arbitrage. La gestion devient plus réactive, mais elle n'est pas pleinement anticipatrice. Un responsable de service décrit cette situation de manière caractéristique :

« Nous avons des indicateurs par service : budget, scolarité, qualité et projets. Ils nous aident à suivre l'activité, mais chacun les regarde de son côté. Quand un indicateur se dégrade, il n'y a pas toujours une instance où l'on croise les données pour décider ensemble. »

Dans la troisième configuration, le contrôle de gestion fonctionne comme un levier d'anticipation et de sécurisation. La différence se joue moins dans la sophistication des outils que dans la stabilité des routines, la mise en discussion des données et l'usage de l'information pour arbitrer. Un secrétaire général décrit l'évolution d'une revue mensuelle autour du tableau de bord :

« Au début, la réunion mensuelle autour du tableau de bord était vécue comme un tribunal. Aujourd'hui, c'est l'espace où l'on discute les blocages : marchés publics, projets de recherche, plateformes numériques. C'est devenu notre espace de gestion des risques, même si on ne l'appelle pas ainsi. »

Tableau 1 : Synthèse comparative des configurations d'usage du contrôle de gestion face au risque

Configuration	Caractéristiques dominantes	Outils et routines	Effet sur le risque et la résilience
Conformité et traçabilité	Priorité donnée au respect des procédures, aux visas et à la justification documentaire.	Reporting budgétaire, contrôles a priori, dossiers justificatifs.	Maîtrise formelle du risque, mais faible anticipation des vulnérabilités opérationnelles.
Performance segmentée	Suivi d'indicateurs d'activité, mais faible croisement entre services et décisions transversales limitées.	Tableaux par service, indicateurs de performance, réunions ponctuelles.	Réactivité accrue, mais anticipation incomplète et apprentissage limité.
Anticipation et sécurisation	Données discutées, seuils d'alerte, arbitrages réguliers et capitalisation après incident.	Revue mensuelles, KPI/KRI, matrices d'arbitrage, retours d'expérience.	Renforcement de l'anticipation, de la coordination et de l'adaptation.

Source : Élaboration de l'auteure à partir des entretiens semi-directifs et de l'analyse documentaire réalisés au deuxième semestre 2025.

3.3. Conditions d'effectivité et rôle des outils de pilotage observés

Les entretiens montrent que la contribution du contrôle de gestion dépend fortement de la gouvernance et de la capacité à faire exister les indicateurs dans la décision. Un responsable du contrôle de gestion le résume ainsi :

« Le contrôle de gestion ne vaut que par l'oreille du doyen. S'il s'en sert pour arbitrer entre les départements, les acteurs prêtent attention aux chiffres. S'il décide seul sans regarder les indicateurs, mon travail devient une simple fonction de secrétariat budgétaire. »

L'apprentissage post-crise constitue une autre condition observable de résilience. Un responsable SI explique qu'un incident numérique a contraint l'établissement à intégrer la sécurité des accès dans les procédures de contrôle interne :

« Après des tentatives de cyberattaque, nous avons revu le suivi des accès. Ce n'est plus seulement technique ; c'est intégré dans nos procédures de contrôle interne. Le choc a forcé un apprentissage qu'on n'arrivait pas à imposer en temps normal. »

Dans ce cadre, deux outils repérés dans le corpus documentaire illustrent la transition d'un pilotage qui suit vers un pilotage qui anticipe. Le premier est un tableau de bord de veille combinant des indicateurs de performance (KPI) et des seuils d'alerte assimilables à des indicateurs de risque (KRI).

Tableau 2 : Tableau de bord de veille utilisé par un établissement universitaire

Axe de pilotage	Indicateur (KPI)	Seuil d'alerte (KRI)	Effet attendu sur la résilience
Pédagogie	Taux d'encadrement réel (étudiants/enseignant)	> 80 étudiants par enseignant	Alerte sur la qualité et le climat social ; anticipation des besoins.
Finances	Délai moyen de paiement fournisseurs	> 60 jours	Alerte sur les prestataires critiques et les risques de rupture de service.
Digital	Indisponibilité des plateformes (LMS/Apogée)	> 2 % par mois	Alerte sur la continuité pédagogique et administrative.

Source : Élaboration de l'auteure à partir des documents de pilotage collectés dans le cadre de l'enquête qualitative.

Le second outil est une matrice d'arbitrage post-choc, mobilisée lors d'une baisse de dotation ou d'un imprévu. Elle classe les activités par criticité et sert de support à la réallocation des ressources. Elle matérialise un principe central de la maîtrise des risques : préserver les processus vitaux — examens, paie, inscriptions, sécurité, continuité numérique — en acceptant des renoncements temporaires sur des activités moins critiques. Elle permet ainsi de transformer l'urgence en arbitrage documenté, plutôt qu'en réaction improvisée.

4. Discussion : hypothèses, apports et conditions de transférabilité

4.1.Mise à l'épreuve des hypothèses

Les résultats soutiennent la première hypothèse : le contrôle de gestion contribue à la maîtrise des risques lorsqu'il organise des routines de décision et d'apprentissage, et non lorsqu'il se limite à produire des tableaux. Cette dynamique rejoint la conception du contrôle comme package cohérent d'instruments et de pratiques (Malmi & Brown, 2008), ainsi que l'idée d'un usage interactif des systèmes de contrôle (Simons, 1995). Ce qui fait levier n'est pas l'indicateur en soi, mais la routine qui le rend opérant : discussion régulière, recherche des causes, priorisation, arbitrage et suivi.

La deuxième hypothèse est également confirmée dans sa logique conditionnelle. Le portage de la gouvernance, la qualité des données, la maturité des systèmes d'information et la culture du risque déterminent l'effectivité du contrôle de gestion. Lorsque ces conditions font défaut,

le dispositif se replie sur la conformité et produit une illusion de maîtrise. Lorsque ces conditions sont présentes, il rend l'incertitude visible, discutable et gouvernable, ce qui alimente les trois dimensions de la résilience : anticipation, coping et adaptation (Duchek, 2020).

4.2. Dialogue avec la littérature : NPM, ERM et universités publiques

Les résultats permettent d'éclairer la tension introduite par les réformes inspirées du New Public Management. En renforçant les objectifs, les indicateurs et la responsabilisation, ces réformes ont introduit dans les universités publiques une logique de performance (Hood, 1991). Cependant, lorsque cette logique se traduit principalement par des obligations de reporting, elle peut renforcer la conformité au détriment du pilotage. Le terrain montre ainsi que la performance ne produit de la résilience que si elle s'accompagne de routines de discussion, de données fiables et d'une gouvernance capable d'arbitrer les priorités.

L'étude dialogue également avec les travaux récents de Bamber et Elezi (2025), qui invitent à dépasser la gestion du risque par catégories pour concevoir l'ERM comme une dynamique transversale connectée aux processus de décision. Les configurations observées confirment cette idée : une cartographie ou un tableau de bord n'a de valeur que s'il influence réellement les décisions budgétaires, numériques, pédagogiques ou organisationnelles. Autrement dit, l'ERM utile dans l'université n'est pas un document supplémentaire ; c'est une capacité d'alignement entre objectifs, responsabilités, données et arbitrages.

4.3. Apports, implications opérationnelles et transférabilité

L'apport principal de l'article est de montrer empiriquement que la relation contrôle de gestion → maîtrise des risques → résilience dépend moins de la sophistication des outils que de leur appropriation managériale. Les universités étudiées deviennent plus résilientes lorsque le pilotage fait parler les indicateurs, installe des seuils d'alerte utiles et transforme l'information en décisions suivies.

Trois implications opérationnelles en découlent. Premièrement, les établissements devraient institutionnaliser des espaces réguliers de revue des tableaux de bord, conçus comme des lieux d'arbitrage et non comme des tribunaux. Deuxièmement, les instruments de performance devraient intégrer explicitement des signaux de vulnérabilité, sur le modèle des tableaux combinant KPI et KRI. Troisièmement, les universités gagneraient à formaliser des mécanismes d'adaptation post-choc, tels que des matrices de criticité, afin que la résilience ne repose pas uniquement sur l'agilité informelle des équipes.

La transférabilité du modèle doit toutefois être discutée avec prudence. Les résultats sont construits à partir d'universités publiques marocaines caractérisées par des contraintes réglementaires, budgétaires et informationnelles spécifiques. Le modèle pourrait être mobilisé dans d'autres contextes, notamment de grandes universités polytechniques, des établissements privés ou des universités d'autres pays africains, mais à condition de tenir compte de la maturité des systèmes d'information, du degré d'autonomie institutionnelle, du mode de financement et des cultures locales de gouvernance. Cette limite ne réduit pas l'apport de l'étude ; elle précise les conditions dans lesquelles son modèle peut être adapté.

5. Conclusion

Cet article a examiné dans quelle mesure, et à quelles conditions, les dispositifs de contrôle de gestion contribuent à la maîtrise des risques et au renforcement de la résilience organisationnelle dans les établissements universitaires publics. À partir d'un terrain qualitatif portant sur dix établissements relevant de trois universités marocaines, fondé sur quinze entretiens semi-directifs et sur l'analyse de documents de pilotage, les résultats montrent que la valeur du contrôle de gestion ne réside pas dans la multiplication des outils, mais dans leur capacité à structurer l'attention, la discussion et l'arbitrage.

La première hypothèse est soutenue : lorsque le contrôle de gestion fonctionne comme un ensemble cohérent de routines et d'instruments, et qu'il est utilisé de manière interactive, il favorise la mise en visibilité des vulnérabilités et une prise en charge plus précoce des tensions. La seconde hypothèse est également confirmée : cette contribution dépend de facteurs organisationnels décisifs, notamment le soutien de la gouvernance, la qualité des données, la maturité des systèmes d'information et l'existence d'une culture de pilotage orientée vers l'apprentissage.

Sur le plan théorique, l'article articule contrôle de gestion, gestion des risques et résilience dans le contexte de l'université publique. Il montre que la résilience ne se décrète pas : elle se construit par des routines qui rendent l'incertitude gouvernable et transforment les épisodes de tension en apprentissages organisationnels. Sur le plan managérial, il invite à renforcer les espaces d'arbitrage, à faire évoluer les tableaux de bord vers des instruments combinant performance et signaux d'alerte, et à formaliser des mécanismes de priorisation post-choc.

L'étude présente toutefois des limites. Son design qualitatif vise une généralisation analytique plutôt que statistique ; il identifie des configurations et des mécanismes plausibles sans mesurer quantitativement leurs effets. Par ailleurs, la résilience étant un processus, une enquête ponctuelle observe mieux les routines et les perceptions que leur évolution dans le temps. Des recherches futures pourraient prolonger ce travail par un suivi longitudinal des crises et des réformes, ainsi que par une validation sur un échantillon élargi d'établissements, afin d'opérationnaliser plus finement la relation entre maturité du pilotage, intégration du risque et capacités de résilience.

Références bibliographiques

- Bamber, C., & Elezi, E. (2025). Enterprise-wide risk management in higher education: Beyond the paradigm of managing risk by categories. *Business Process Management Journal*, 31(6), 2204–2228.
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101.
- Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management—Integrating with strategy and performance*. COSO.
- Duchek, S. (2020). Organizational resilience: A capability-based conceptualization. *Business Research*, 13(1), 215–246.
- Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review*, 14(4), 532–550.
- Hood, C. (1991). A public management for all seasons? *Public Administration*, 69(1), 3–19.
- International Organization for Standardization. (2018). *ISO 31000:2018 Risk management—Guidelines*. ISO.
- Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. SAGE.
- Malmi, T., & Brown, D. A. (2008). Management control systems as a package—Opportunities, challenges and research directions. *Management Accounting Research*, 19(4), 287–300.
- Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook* (3rd ed.). SAGE.
- Simons, R. (1995). *Levers of control: How managers use innovative control systems to drive strategic renewal*. Harvard Business School Press.
- University Risk Management and Insurance Association. (2023). *URMIA enterprise risk management resource for higher education*. <https://www.urmia.org/viewdocument/enterprise-risk-management-resource>
- Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). SAGE.

CHAPITRE 8: *Intégration de la gestion des risques dans la planification stratégique publique au Maroc : Cadres, mécanismes et effets sur la gouvernance*

BAKHTAOUI MIMOUN

Docteur en Economie et Gestion, Faculté des Sciences Juridiques Economiques et Sociales
Université Mohamed Premier – Oujda- bakhtaouimimoun@gmail.com

TBATIT ABDELHAMID

Doctorant en Economie et Gestion, Ecole Nationale de Commerce et de Gestion, Université
Mohamed Premier – Oujda-abdelhamid.tbatit@gmail.com

Le 8 septembre 2023, un séisme de magnitude 6,8 a frappé la province d'Al Haouz, dans le Haut Atlas marocain, rappelant avec une brutalité particulière la vulnérabilité structurelle face aux aléas naturels. Cet événement n'est pourtant pas isolé dans la trajectoire récente de l'action publique marocaine : la gestion de la pandémie de Covid-19, la récurrence des épisodes de stress hydrique, l'exposition croissante aux dérèglements climatiques et la volatilité des grands équilibres budgétaires ont, chacun à leur manière, posé à l'État la même question lancinante — celle de sa capacité à anticiper l'incertain plutôt qu'à seulement y réagir. Cette question n'est pas nouvelle dans son principe, mais elle a pris, depuis le milieu des années 2010, une tournure résolument institutionnelle. La gestion des risques n'y est plus seulement un savoir-faire opérationnel mobilisé dans l'urgence ; elle tend à devenir un référentiel d'action publique à part entière, susceptible d'irriguer en amont les dispositifs de planification stratégique de l'État.

Cette évolution s'inscrit dans une double dynamique. D'une part, la planification publique marocaine a connu, depuis l'indépendance, plusieurs mues successives : des plans quinquennaux de développement à la multiplication, depuis le tournant des années 2000, de stratégies sectorielles ambitieuses — Plan Maroc Vert, Plan d'accélération industrielle, visions touristiques successives —, puis, à partir de 2015, à une rationalisation budgétaire axée sur la performance portée par la loi organique relative à la loi de finances. D'autre part, la gestion des risques s'est progressivement institutionnalisée comme champ autonome de l'action publique, à travers la création d'organes dédiés, l'adoption de référentiels internationaux et un dialogue suivi avec des organisations telles que l'Organisation de coopération et de développement économiques (OCDE) ou la Banque mondiale. Ces deux trajectoires — celle de la planification stratégique et celle de la gestion des risques — se sont longtemps développées de manière relativement disjointe, chacune répondant à sa propre logique institutionnelle et à son propre calendrier de réforme.

C'est précisément à l'endroit de leur rencontre que se situe la problématique de cet article. Comment la gestion des risques s'intègre-t-elle, à travers quels cadres juridico-institutionnels et quels mécanismes opérationnels, dans les processus de planification stratégique de l'action publique marocaine ? Et quels effets, positifs ou ambivalents, cette intégration produit-elle sur la qualité de la gouvernance publique, entendue ici dans ses dimensions de transparence, de redevabilité et de résilience institutionnelle ? Cette interrogation centrale se décline en trois questions plus spécifiques, qui structurent la démarche empirique de l'article : quels sont les cadres juridiques et institutionnels qui portent, en droit marocain, cette articulation entre risque et stratégie ? Quels mécanismes opérationnels concrets la traduisent dans la pratique administrative ? Et dans quelle mesure cette intégration formelle se traduit-elle par une appropriation managériale réelle, ou se limite-t-elle à un exercice de conformité aux standards internationaux ?

L'intérêt de cette interrogation est double. Sur le plan théorique, elle permet de mettre à l'épreuve, dans un contexte d'économie émergente où la tradition administrative reste marquée par une forte centralisation, des cadres conceptuels — gouvernance du risque, néo-institutionnalisme, critique de la planification stratégique — majoritairement élaborés à partir de l'expérience des pays de l'OCDE les plus anciennement industrialisés. Sur le plan managérial, elle offre aux décideurs publics, aux chercheurs et aux étudiants en administration

publique une grille de lecture susceptible d'éclairer les marges de progression d'un chantier de réforme encore en cours. L'article s'organise en six mouvements principaux. Une revue de la littérature précise les fondements théoriques mobilisés (section 2). Le positionnement épistémologique et la démarche méthodologique sont ensuite explicités (section 3). L'étude empirique restitue d'abord les cadres et mécanismes observés dans le cas marocain (section 4), avant d'en proposer une analyse critique au regard de leurs effets sur la gouvernance (section 5). Une discussion remet ces résultats en perspective théorique (section 6), avant que ne soient formulées des recommandations (section 7) et des perspectives de recherche (section 8).

2. Cadre théorique et revue de la littérature

2.1 Le risque et sa gestion : généalogie d'une notion plurielle

La notion de risque ne renvoie pas à une réalité univoque. Dans sa généalogie la plus ancienne, héritée des mathématiques des probabilités et des pratiques assurantielles, le risque est conçu comme un aléa objectivable, mesurable par la combinaison d'une probabilité d'occurrence et d'une gravité d'impact. Cette acception « actuarielle » a longtemps dominé la gestion publique des risques naturels et financiers. Elle a cependant été profondément renouvelée par les travaux de sociologie du risque qui, à partir des années 1980, ont mis en évidence le caractère socialement construit de la perception et de la hiérarchisation des risques. Beck (2001 [1986]) montre ainsi que les sociétés contemporaines, qu'il qualifie de « sociétés du risque », sont confrontées à des dangers largement produits par leur propre développement technique et industriel, et que la définition de ce qui constitue un risque acceptable relève autant d'arbitrages sociaux et politiques que de calculs probabilistes⁶¹. Dans une veine convergente, Douglas et Wildavsky (1982) montrent que la perception du risque varie selon les cultures organisationnelles et les rapports de pouvoir, ce qui invite à se méfier d'une lecture purement technique des dispositifs de gestion des risques dans l'administration⁶².

Cette tension entre approche technique et approche socialement construite se retrouve dans les référentiels managériaux qui structurent aujourd'hui la pratique organisationnelle. La norme ISO 31000, dans sa version de 2018, définit le risque comme l'effet de l'incertitude sur l'atteinte des objectifs, et recommande que le management du risque soit pleinement intégré à la gouvernance, à la stratégie et à la planification de toute organisation, plutôt que traité comme une fonction périphérique⁶³. Le référentiel COSO relatif au management des risques de l'entreprise, dans sa refonte de 2017, pousse cette logique plus loin encore en articulant explicitement la gestion des risques à la définition même de la stratégie et à l'évaluation de la performance organisationnelle, à travers cinq composantes : gouvernance et culture, stratégie

⁶¹Beck, U. (2001 [1986]). *La société du risque : sur la voie d'une autre modernité*. Paris, Aubier.

⁶²Douglas, M., & Wildavsky, A. (1982). *Risk and Culture: An Essay on the Selection of Technological and Environmental Dangers*. Berkeley, University of California Press.

⁶³International Organization for Standardization [ISO] (2018). *ISO 31000:2018 — Management du risque : lignes directrices*. Genève, ISO.

et fixation des objectifs, performance, révision, information et communication⁶⁴. Transposés au secteur public, ces référentiels invitent à distinguer plusieurs catégories de risques — risques stratégiques, financiers, opérationnels, de conformité, réputationnels — auxquelles s'ajoute, dans des pays comme le Maroc, la catégorie spécifique des risques majeurs ou de catastrophe, objet en 2014 d'une recommandation dédiée du Conseil de l'OCDE⁶⁵.

Cette diffusion normative n'est cependant pas sans susciter une littérature critique. Power (2004) avance la thèse d'un « management du risque généralisé », selon laquelle la multiplication des dispositifs formels de gestion des risques dans les organisations contemporaines répond autant à une logique défensive de mise en conformité et de protection contre la mise en cause de la responsabilité des dirigeants qu'à une réelle amélioration de la prise de décision⁶⁶. Cette mise en garde constitue un fil conducteur important de la présente analyse, qui s'attachera précisément à distinguer, dans le cas marocain, ce qui relève d'une appropriation managériale substantielle de ce qui pourrait davantage s'apparenter à un exercice de mise en forme institutionnelle.

2.2 Planification stratégique publique : entre rationalisation et incertitude

La planification stratégique publique désigne le processus par lequel une organisation publique définit ses objectifs de moyen et long termes, mobilise les moyens nécessaires à leur réalisation et organise leur séquençage dans le temps. Cette définition, en apparence consensuelle, recouvre en réalité un paradigme largement rationaliste, hérité de la planification économique d'après-guerre, qui présuppose un environnement suffisamment stable et connaissable pour qu'un diagnostic initial, des objectifs chiffrés et un plan d'action puissent être arrêtés ex ante puis simplement mis en œuvre et contrôlés. Mintzberg (1994) a montré, de manière désormais classique, les limites de ce paradigme : la planification formelle tend à produire une illusion de contrôle sur un environnement par nature incertain, et peut se substituer à la réflexion stratégique véritable plutôt que la nourrir⁶⁷.

L'avènement du Nouveau Management Public, dont Hood (1991) a proposé l'une des formalisations les plus citées, a partiellement déplacé ce paradigme en substituant au contrôle a priori des moyens un pilotage par les objectifs et les résultats, assorti d'une obligation de reddition des comptes⁶⁸. Cette doctrine trouve, dans le cas marocain, une traduction directe dans la loi organique relative à la loi de finances, dont l'architecture — projets de performance, indicateurs, programmation budgétaire triennale — relève précisément d'une logique de

⁶⁴Committee of Sponsoring Organizations of the Treadway Commission [COSO] (2017). *Enterprise Risk Management — Integrating with Strategy and Performance*. New York, COSO.

⁶⁵Organisation de coopération et de développement économiques [OCDE] (2014). *Recommandation du Conseil sur la gouvernance des risques majeurs*. Paris, OCDE.

⁶⁶Power, M. (2004). *The Risk Management of Everything: Rethinking the Politics of Uncertainty*. Londres, Demos.

⁶⁷Mintzberg, H. (1994). *The Rise and Fall of Strategic Planning*. New York, Free Press.

⁶⁸Hood, C. (1991). A public management for all seasons? *Public Administration*, 69(1), 3-19.

pilotage par les résultats⁶⁹. Or cette logique, en obligeant chaque gestionnaire public à formuler explicitement les objectifs poursuivis et à en mesurer périodiquement l'atteinte, crée structurellement les conditions d'une identification des risques pesant sur cette atteinte : tout écart significatif entre objectif fixé et résultat observé constitue, de fait, la matérialisation d'un risque non anticipé ou insuffisamment maîtrisé. La rencontre entre planification stratégique et gestion des risques peut ainsi se lire comme l'aboutissement logique, bien que rarement explicité comme tel, de la généralisation d'une gestion publique axée sur la performance.

2.3 Gouvernance publique, risque et résilience : une articulation conceptuelle

La gouvernance publique renvoie aux processus, formels et informels, par lesquels une pluralité d'acteurs — autorités publiques, partenaires techniques et financiers, collectivités territoriales, société civile — coordonnent leur action en vue de la définition et de la mise en œuvre des politiques publiques. Les critères usuellement mobilisés pour en apprécier la qualité — transparence, redevabilité, participation, efficacité, état de droit — recoupent largement les effets que l'on peut attendre d'une intégration réussie de la gestion des risques dans la planification stratégique.

Le cadre de la gouvernance du risque, proposé notamment par Renn (2008) dans le prolongement des travaux du Conseil international pour la gouvernance des risques, offre à cet égard une passerelle conceptuelle précieuse⁷⁰. Il invite à ne pas réduire la gestion des risques à sa seule dimension technique d'évaluation probabiliste, mais à l'articuler explicitement à des exigences de légitimité, de participation des parties prenantes et de communication transparente sur les arbitrages opérés. Sous cet angle, un dispositif de gestion des risques bien intégré à la planification stratégique devrait, en toute logique, renforcer simultanément la performance de l'action publique et sa gouvernance démocratique.

Cette articulation théorique gagne à être complétée par un second cadre, davantage critique, issu du néo-institutionnalisme sociologique. DiMaggio et Powell (1983) montrent que les organisations, et singulièrement les organisations publiques exposées à la pression de bailleurs de fonds et de standards internationaux, tendent à adopter des structures formelles similaires sous l'effet de mécanismes d'isomorphisme coercitif, mimétique ou normatif, indépendamment de leur efficacité fonctionnelle propre⁷¹. Meyer et Rowan (1977) prolongent cette analyse par le concept de découplage, désignant l'écart possible entre les structures formelles adoptées à des fins de légitimité — chartes, observatoires, cartographies de risques — et les pratiques

⁶⁹Royaume du Maroc (2015a). *Loi organique n° 130-13 relative à la loi de finances*, promulguée par le dahir n° 1-15-62 du 2 juin 2015, Bulletin officiel n° 3107 ; Royaume du Maroc (2015b). *Décret n° 2-15-426 du 15 juillet 2015 relatif à l'élaboration et à l'exécution des lois de finances*.

⁷⁰Renn, O. (2008). *Risk Governance: Coping with Uncertainty in a Complex World*. Londres, Earthscan.

⁷¹DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147-160.

effectives de gestion au quotidien⁷². Ce double cadre conceptuel — gouvernance du risque, d’une part, néo-institutionnalisme et découplage, d’autre part — fournit la grille interprétative à partir de laquelle les résultats empiriques de cet article seront discutés.

2.4 Modèle d’analyse retenu

La synthèse de cette revue de littérature conduit à retenir, pour l’analyse empirique, une grille structurée autour de trois dimensions complémentaires. La première porte sur les cadres juridico-institutionnels, c’est-à-dire les textes de loi, décrets et dispositifs organisationnels qui consacrent, explicitement ou implicitement, une obligation ou une incitation à intégrer le risque dans la planification de l’action publique. La seconde porte sur les mécanismes opérationnels par lesquels cette intégration se traduit concrètement : cartographies des risques, audits fondés sur le risque, indicateurs de performance, dispositifs d’alerte précoce, mécanismes de financement contingent. La troisième porte enfin sur les effets de cette intégration sur la gouvernance, entendus à la fois dans leur dimension positive — transparence, redevabilité, résilience institutionnelle — et dans leur dimension plus ambivalente, relative au risque de découplage entre dispositifs formels et appropriation managériale réelle. Cette grille à trois dimensions structure directement l’organisation des sections empiriques qui suivent.

3. Positionnement épistémologique et démarche méthodologique

3.1 Posture épistémologique

La présente recherche adopte une posture épistémologique interprétativiste. Ce choix se justifie par la nature même de l’objet étudié : la façon dont les acteurs administratifs marocains définissent, formalisent et donnent du sens à la notion de risque au sein des processus de planification stratégique relève d’une construction sociale et institutionnelle, et non d’un phénomène dont l’existence serait indépendante de l’observateur et réductible à des lois causales générales. À la différence d’une posture positiviste, qui chercherait à tester, sur la base d’indicateurs quantitatifs préétablis, des hypothèses formulées a priori sur la relation entre gestion des risques et performance de la gouvernance, la posture retenue ici vise plutôt à comprendre, à partir des traces documentaires laissées par les institutions elles-mêmes, la manière dont s’est construite, dans le temps et au sein de plusieurs champs sectoriels, l’articulation entre risque et stratégie. Cette option rejoint la distinction classique opérée par Guba et Lincoln (1994) entre paradigmes positiviste et naturaliste, ce dernier reconnaissant la pluralité des réalités construites par les acteurs et la nécessité, pour le chercheur, de s’immerger

⁷²Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: formal structure as myth and ceremony. *American Journal of Sociology*, 83(2), 340-363.

dans le contexte spécifique de son terrain plutôt que de chercher à en abstraire des régularités universelles⁷³.

3.2 Stratégie de recherche : étude de cas qualitative

Conformément à cette posture, la recherche mobilise une stratégie d'étude de cas qualitative, au sens défini par Yin (2018), centrée sur le cas unique du Maroc mais déclinée en plusieurs unités d'analyse imbriquées : le champ budgétaro-financier, le champ de la gestion des risques de catastrophes naturelles, et le champ de la planification stratégique de développement portée par le Nouveau Modèle de Développement. Ce choix méthodologique se justifie par la nature même des questions de recherche posées — des questions de type « comment » et « avec quels effets », pour lesquelles l'étude de cas constitue, selon une tradition méthodologique bien établie, un dispositif particulièrement adapté lorsque le phénomène étudié est fortement contextualisé et que les frontières entre le phénomène et son contexte ne sont pas nettement tranchées⁷⁴.

3.3 Corpus documentaire mobilisé

Le corpus documentaire rassemblé pour cette recherche comprend trois catégories de sources. La première regroupe les textes juridiques et institutionnels marocains directement relatifs à la planification stratégique et à la gestion des risques : la loi organique n° 130-13 relative à la loi de finances et son décret d'application, la Stratégie nationale de gestion des risques des catastrophes naturelles 2020-2030, ainsi que le rapport général de la Commission spéciale sur le modèle de développement. La seconde regroupe des rapports d'instances nationales de contrôle et de consultation, notamment les communications du ministère de l'Économie et des Finances relatives à l'évaluation PEFA 2023 et le rapport du Conseil économique, social et environnemental consacré à la gestion des risques de catastrophes naturelles. La troisième regroupe des évaluations indépendantes produites par des organisations internationales, en particulier les examens successifs de l'OCDE sur la gouvernance publique et la gestion des risques au Maroc, ainsi qu'un rapport de la Banque mondiale portant sur la résilience aux catastrophes naturelles. Le tableau 1, présenté en section 4, synthétise les principales composantes institutionnelles associées à ce corpus.

Le choix de privilégier des sources documentaires officielles, plutôt que des données primaires recueillies par entretien, répond à une double considération. D'une part, ces documents constituent eux-mêmes des traces directes du processus d'institutionnalisation étudié : ils sont la matérialisation officielle de l'articulation entre risque et stratégie, et non une simple description de seconde main de cette articulation. D'autre part, l'accès à des données primaires internes à l'administration marocaine — comptes rendus de réunions, dossiers d'audit non

⁷³Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. Dans N. K. Denzin & Y. S. Lincoln (dir.), *Handbook of Qualitative Research* (p. 105-117). Thousand Oaks, Sage.

⁷⁴Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods* (6e éd.). Thousand Oaks, Sage.

publics, entretiens avec les gestionnaires de risques sectoriels — s’est révélé, dans le cadre temporel de cette recherche, difficilement praticable, ce qui constitue l’une des limites assumées de la démarche, discutée plus loin.

3.4 Méthode d’analyse des données

L’analyse du corpus a procédé par une analyse de contenu thématique, dans la tradition établie par Bardin (1977), organisée en trois temps⁷⁵. Une première lecture flottante de l’ensemble des documents a permis de repérer les occurrences et les contextes d’emploi des notions de risque, de stratégie et de gouvernance. Une seconde étape a procédé au codage thématique de ces occurrences selon les trois dimensions du modèle d’analyse présenté en section 2.4 — cadres juridico-institutionnels, mécanismes opérationnels, effets sur la gouvernance —, en distinguant, au sein de chaque dimension, des sous-thèmes récurrents tels que l’audit fondé sur le risque, la cartographie des risques naturels, ou la résilience institutionnelle. Une troisième étape a procédé à une mise en regard systématique des documents nationaux et des évaluations internationales, dans une logique de triangulation destinée à limiter le biais d’auto-évaluation inhérent aux sources produites par les institutions elles-mêmes étudiées : lorsque le diagnostic porté par un document marocain de nature programmatique rencontrait, ou au contraire contredisait, celui porté par une évaluation indépendante telle qu’un examen de l’OCDE, cet écart a été retenu comme une donnée interprétative à part entière.

3.5 Limites méthodologiques

Cette démarche présente des limites qu’il convient d’assumer explicitement. L’absence de données primaires de terrain — entretiens avec les gestionnaires de risques au sein des ministères sectoriels, enquêtes auprès des cadres territoriaux chargés de la mise en œuvre des stratégies nationales — restreint la portée des conclusions au niveau formel et déclaré de l’intégration étudiée, sans permettre de documenter directement les pratiques managériales quotidiennes. Le corpus repose en outre, pour une part substantielle, sur des documents produits par les institutions mêmes dont l’action est analysée, ce qui appelle une lecture prudente, nuancée en partie par la triangulation avec des sources internationales indépendantes mais non entièrement neutralisée par celle-ci. Enfin, la recherche porte sur un objet en évolution rapide : certains constats relatifs à des réformes encore en cours de déploiement pourraient se trouver datés à brève échéance. Ces limites, plutôt que d’invalider la démarche, en délimitent la portée et appellent, comme il sera précisé en conclusion, des recherches complémentaires de nature empirique.

⁷⁵Bardin, L. (1977). *L’analyse de contenu*. Paris, Presses universitaires de France.

4. Cadres et mécanismes d'intégration de la gestion des risques dans la planification stratégique publique au Maroc

4.1 Le vecteur budgétaro-légal : la loi organique relative à la loi de finances

La loi organique n° 130-13 relative à la loi de finances, promulguée par le dahir du 2 juin 2015 et précisée par le décret n° 2-15-426 du 15 juillet de la même année, constitue le premier vecteur juridique par lequel une logique de gestion des risques s'est insérée, sans toujours en porter explicitement le nom, dans la planification de l'action publique marocaine⁷⁶. Inscrite dans le sillage de la Constitution de 2011, cette réforme a substitué à un contrôle a priori centré sur la régularité des moyens un pilotage par la performance, structuré autour de projets de performance assortis d'objectifs et d'indicateurs, d'une programmation budgétaire triennale et d'un renforcement des principes de reddition des comptes et d'évaluation⁷⁷. Cette architecture, bien qu'élaborée dans un vocabulaire essentiellement budgétaire, comporte une dimension de gestion des risques intrinsèque : en obligeant chaque département ministériel à documenter les résultats attendus de son action et à en rendre compte périodiquement, elle crée les conditions d'une détection précoce des écarts entre objectifs et réalisations, écarts qui constituent la trace la plus immédiate de risques non maîtrisés. La circulaire annuelle relative à la programmation budgétaire triennale, dont celle adressée par le Chef du gouvernement aux départements ministériels pour la période 2025-2027, prolonge cette logique en exigeant des administrations qu'elles anticipent, au-delà du seul exercice budgétaire annuel, la trajectoire pluriannuelle de leurs objectifs et des moyens afférents.

4.2 L'architecture du contrôle et de l'audit : Inspection générale des finances, Trésorerie générale du Royaume et Cour des comptes

Au-delà du cadre budgétaire, l'architecture marocaine de contrôle et d'audit a connu, au cours de la dernière décennie, une mutation significative vers une logique explicitement fondée sur le risque. L'Inspection générale des finances, corps de contrôle supérieur placé sous l'autorité du ministère de l'Économie et des Finances depuis sa création en 1960, a ainsi fait évoluer ses méthodes de programmation des missions d'audit et d'inspection vers une approche dite d'audit fondé sur les risques, consistant à établir une cartographie des risques pesant sur les administrations et organismes publics afin de concentrer les missions de contrôle sur les zones

⁷⁶Royaume du Maroc (2015a). *Loi organique n° 130-13 relative à la loi de finances*, promulguée par le dahir n° 1-15-62 du 2 juin 2015, Bulletin officiel n° 3107 ; Royaume du Maroc (2015b). *Décret n° 2-15-426 du 15 juillet 2015 relatif à l'élaboration et à l'exécution des lois de finances*.

⁷⁷Bensouda, N. (2012). *La réforme de la loi organique des finances : vers un nouveau modèle de gestion des finances publiques*. Communication, Association des membres de l'Inspection générale des finances, Rabat.

de vulnérabilité les plus élevées plutôt que de procéder selon une logique exhaustive ou aléatoire héritée d'une tradition de contrôle plus strictement légaliste. Cette réorientation méthodologique coexiste avec le rôle constitutionnellement consacré de la Cour des comptes, dont la crédibilité a été explicitement soulignée comme un point fort du système marocain de gestion des finances publiques par l'évaluation indépendante conduite dans le cadre du programme international PEFA en 2023⁷⁸.

Cette évaluation PEFA 2023, troisième exercice de ce type conduit au Maroc après ceux de 2009 et de 2016, mérite à cet égard une attention particulière. Conduite selon une méthodologie simplifiée dite « PEFA agile » et financée conjointement par la Banque mondiale, la Banque africaine de développement, l'Union européenne et l'Agence française de développement, elle a porté sur trente et un indicateurs regroupés en sept piliers couvrant la discipline budgétaire, l'allocation stratégique des ressources et l'efficacité de l'utilisation des ressources pour la prestation des services. Plus de soixante pour cent de l'ensemble des indicateurs examinés se classent désormais dans les catégories supérieures de notation, signe d'une dynamique d'amélioration soutenue au fil des trois exercices, même si des marges de progrès demeurent identifiées, notamment quant aux délais de publication de la loi de règlement et à la programmation des projets d'investissement. Cette progression mesurée, sur quinze années et trois exercices d'évaluation indépendante, constitue l'un des indices les plus tangibles dont dispose la présente recherche pour apprécier les effets concrets — et non simplement déclaratifs — de la rationalisation budgétaire engagée depuis la loi organique de 2015⁷⁹.

4.3 La gestion des risques de catastrophes naturelles : une politique sectorielle pionnière

C'est cependant dans le champ spécifique de la gestion des risques de catastrophes naturelles que l'articulation entre gestion des risques et planification stratégique apparaît, dans le cas marocain, la plus aboutie. Cette politique trouve son origine dans le séisme d'Al Hoceima de 2004, dont les insuffisances de gestion de crise avaient été explicitement pointées au plus haut niveau de l'État, ouvrant la voie à un long travail de capitalisation des retours d'expérience et, à partir de 2008, à un partenariat soutenu avec la Banque mondiale⁸⁰. Cette maturation institutionnelle a connu deux jalons majeurs. En 2020, le ministère de l'Intérieur a créé une Direction de la gestion des risques naturels, désormais en charge d'un mandat institutionnel précis et mobilisant aujourd'hui plus de quatre-vingts collaborateurs à plein temps. La même année, le Conseil du gouvernement a examiné la Stratégie nationale de gestion des risques des catastrophes naturelles 2020-2030, structurée autour de trois objectifs thématiques — améliorer la connaissance et l'évaluation des risques, notamment par la création d'un Observatoire national des risques naturels ; promouvoir la prévention des risques pour renforcer la résilience

⁷⁸Ministère de l'Économie et des Finances du Royaume du Maroc (2024). *Atelier de dissémination des résultats de l'évaluation PEFA 2023*. Rabat, MEF.

⁷⁹Ministère de l'Économie et des Finances du Royaume du Maroc (2024). *Atelier de dissémination des résultats de l'évaluation PEFA 2023*. Rabat, MEF.

⁸⁰Banque mondiale (2024). *Des catastrophes aux opportunités : construire un avenir résilient au Maroc*. Washington, World Bank Group.

des populations et des territoires ; et améliorer la préparation aux catastrophes pour un relèvement rapide et une reconstruction efficace — et de deux objectifs transversaux portant sur le renforcement de la gouvernance de la gestion des risques et la promotion de la recherche scientifique et de la coopération internationale. Ces objectifs sont déclinés en cinq axes stratégiques et dix-huit programmes et projets opérationnels⁸¹.

La portée concrète de cette stratégie se mesure à l'aune de réalisations tangibles plutôt que de seules intentions programmatiques. Un système de financement hybride des risques de catastrophe a été mis en place, combinant un régime d'assurance privé couvrant l'ensemble de la population marocaine à un fonds public de solidarité ; ce dispositif a permis de mobiliser l'équivalent de trois cents millions de dollars dans les mois ayant suivi le séisme d'Al Haouz survenu en 2023. Par ailleurs, quatre provinces servent aujourd'hui de terrain pilote à un dispositif d'alerte précoce contre les crues, dont la couverture touche directement environ deux cent quarante mille habitants⁸². Ces réalisations, documentées par un rapport de la Banque mondiale publié en 2024, illustrent une transformation effective de la posture de l'État, passée d'une logique réactive et post-catastrophe à une logique anticipative, intégrée en amont dans la planification stratégique du secteur.

Le rapport publié en 2024 par le Conseil économique, social et environnemental sur la gestion des risques de catastrophes naturelles apporte cependant un éclairage plus nuancé sur cette même politique⁸³. S'il reconnaît que la stratégie nationale a institué un dispositif de gouvernance intégré et participatif destiné à unifier les efforts des nombreuses entités impliquées dans la prévention et la gestion des crises, il souligne que sa mise en œuvre se heurte, sur le terrain, à des obstacles tenant notamment à une circulation insuffisante de l'information et à des disparités dans le niveau de préparation des acteurs locaux. Le Conseil recommande, en conséquence, de généraliser, en l'adaptant aux réalités locales, le contenu de la stratégie nationale dans les documents de planification territoriale — plans de développement régional, plans de développement provincial, plans d'aménagement communal — et d'accélérer la territorialisation de l'Observatoire national des risques naturels. Cette nuance, émanant d'une instance consultative indépendante, invite à ne pas confondre la maturité du cadre stratégique national, indéniable, avec la maturité de son appropriation à l'échelle des territoires, sur laquelle des progrès demeurent attendus.

4.4 Le Nouveau Modèle de Développement : la résilience comme horizon stratégique

À un niveau de généralité supérieur à celui des politiques sectorielles examinées jusqu'ici, le Nouveau Modèle de Développement constitue le cadre stratégique le plus ambitieux dans lequel

⁸¹Banque mondiale (2024). *Des catastrophes aux opportunités : construire un avenir résilient au Maroc*. Washington, World Bank Group.

⁸²Banque mondiale (2024). *Des catastrophes aux opportunités : construire un avenir résilient au Maroc*. Washington, World Bank Group.

⁸³Conseil économique, social et environnemental [CESE] (2024). *Pour une gestion efficace et proactive des risques des catastrophes naturelles : rôles et capacités des acteurs territoriaux*. Rabat, CESE.

le Maroc ait, à ce jour, formulé sa vision de long terme. Issu des travaux de la Commission spéciale sur le modèle de développement, instituée à l'initiative royale en 2019 et présidée par Chakib Benmoussa, ce rapport est le fruit d'une démarche d'écoute et de consultation conduite entre janvier 2020 et avril 2021 auprès de l'ensemble des composantes politiques, économiques et sociales du pays. Remis en mai 2021 sous l'intitulé « Le Nouveau Modèle de Développement — Libérer les énergies et restaurer la confiance pour accélérer la marche vers le progrès et la prospérité pour tous », il s'organise en trois parties consacrées respectivement au diagnostic du Maroc contemporain et du monde à venir, à la formulation du nouveau modèle proposé, et aux leviers de changement permettant sa mise en œuvre⁸⁴.

Ce rapport présente un intérêt particulier pour la présente analyse à un double titre. D'une part, sa phase de diagnostic procède elle-même d'une démarche d'identification des vulnérabilités structurelles du modèle de développement antérieur — économiques, sociales, territoriales — qui s'apparente, dans sa logique sinon dans son vocabulaire, à un exercice d'évaluation des risques systémiques pesant sur la trajectoire du pays. D'autre part, parmi les quatre axes de transformation retenus pour l'horizon 2035, celui relatif au capital humain et à l'inclusion sociale appelle explicitement la consolidation d'un socle de protection sociale renforçant, selon les termes mêmes du rapport, la résilience et l'inclusion des citoyens. La résilience apparaît ainsi, pour la première fois à ce niveau de généralité stratégique, comme une finalité explicitement assignée à l'action publique, et non plus seulement comme une propriété recherchée dans des politiques sectorielles spécifiques telles que la gestion des risques naturels. La proposition d'un Pacte national pour le développement et d'un mécanisme de suivi destiné à impulser la mise en œuvre des réformes préconisées peut elle-même se lire comme un dispositif de prévention d'un risque récurrent dans la trajectoire marocaine, identifié par la Commission elle-même : celui de la discontinuité des réformes au gré des cycles politiques et administratifs⁸⁵.

4.5 L'inscription internationale : l'adhésion du Maroc aux standards de gouvernance des risques de l'OCDE

L'intégration de la gestion des risques dans la planification stratégique marocaine ne s'est pas construite de manière endogène. Elle s'est largement appuyée sur un dialogue soutenu avec l'OCDE, engagé dès 2014 lorsque le Maroc a adhéré à la Recommandation du Conseil de l'OCDE sur la gouvernance des risques majeurs au moment même de son adoption par les ministres des pays membres⁸⁶. Cette adhésion a été précédée d'un atelier de travail conjoint,

⁸⁴Commission spéciale sur le modèle de développement [CSMD] (2021). *Le Nouveau Modèle de Développement : libérer les énergies et restaurer la confiance pour accélérer la marche vers le progrès et la prospérité pour tous — Rapport général*. Rabat, CSMD.

⁸⁵Commission spéciale sur le modèle de développement [CSMD] (2021). *Le Nouveau Modèle de Développement : libérer les énergies et restaurer la confiance pour accélérer la marche vers le progrès et la prospérité pour tous — Rapport général*. Rabat, CSMD.

⁸⁶Organisation de coopération et de développement économiques [OCDE] (2014). *Recommandation du Conseil sur la gouvernance des risques majeurs*. Paris, OCDE.

organisé en février 2014 par le ministère des Affaires générales et de la Gouvernance et le ministère de l'Intérieur, qui a permis d'arrêter les termes de référence d'une revue par les pairs de la politique marocaine de gestion des risques. Cette revue, publiée par l'OCDE en 2016, a analysé l'action des multiples acteurs impliqués — administration centrale, collectivités territoriales, organismes de recherche, secteur privé et société civile — sur l'ensemble du cycle de gestion des risques, de l'évaluation à la reconstruction, en portant une attention particulière aux questions de gouvernance, de coordination entre acteurs et d'inclusion des populations concernées⁸⁷.

Ce dialogue s'est poursuivi par un diagnostic d'intégrité publique, publié par l'OCDE en 2018, qui a recommandé au Maroc d'appliquer un cadre de contrôle et de gestion des risques explicitement orienté vers la protection de l'intégrité au sein des organisations du secteur public, en évaluant l'environnement de contrôle interne marocain à l'aune des standards internationaux⁸⁸. Un rapport régional publié par l'OCDE en 2019, portant sur le contrôle interne et la gestion des risques pour l'intégrité publique dans sept économies du Moyen-Orient et d'Afrique du Nord dont le Maroc, a mis en évidence un obstacle structurel commun à ces économies : une tradition administrative centralisée et hiérarchique, organisée selon une logique ministérielle sectorielle, qui complique l'adoption simultanée d'une gestion par les résultats, d'une allocation rationnelle des ressources et d'une maîtrise effective des risques par les gestionnaires de terrain⁸⁹. Enfin, l'examen le plus récent de la gouvernance publique marocaine conduit par l'OCDE, publié en 2023 sous le titre « Pour une administration résiliente au service des citoyens », recommande explicitement que le Maroc renforce une approche stratégique de la gestion des risques au niveau du contrôle et de l'audit internes, aux côtés d'autres priorités telles que la protection des lanceurs d'alerte et la transparence des activités d'influence⁹⁰.

Cette succession d'engagements, échelonnée sur près d'une décennie, dessine un processus progressif et largement échafaudé depuis l'extérieur d'internalisation des normes internationales de gouvernance du risque, dont la dynamique mérite d'être interrogée à l'aune des mécanismes d'isomorphisme normatif et mimétique évoqués en section 2.3 : la lecture proposée en section 5 reviendra sur cette hypothèse.

Tableau 1. Synthèse du cadre institutionnel marocain d'intégration de la gestion des risques dans la planification stratégique publique

⁸⁷OCDE (2016). *L'étude de l'OCDE sur la gestion des risques au Maroc*. Paris, Éditions OCDE.

⁸⁸OCDE (2018). *Examens de l'OCDE sur la gouvernance publique : diagnostic d'intégrité au Maroc*. Paris, Éditions OCDE.

⁸⁹OCDE (2019). *Examens de l'OCDE sur la gouvernance publique : contrôle interne et gestion des risques pour l'intégrité publique au Moyen-Orient et en Afrique du Nord*. Paris, Éditions OCDE.

⁹⁰OCDE (2023). *Examens de l'OCDE sur la gouvernance publique : Maroc — pour une administration résiliente au service des citoyens*. Paris, Éditions OCDE.

Niveau	Acteur ou dispositif	Texte ou référence principale	Contribution à l'intégration risque-stratégie
Budgétaire-légal	Ministère de l'Économie et des Finances, Direction du Budget	Loi organique n° 130-13 (2015), décret n° 2-15-426	Pilotage par la performance, programmation triennale, identification des écarts objectifs-résultats
Contrôle et audit	Inspection générale des finances	Approche d'audit fondé sur les risques	Cartographie et priorisation des missions de contrôle
Contrôle supérieur	Cour des comptes	Constitution de 2011 ; évaluation PEFA 2023	Certification, crédibilité reconnue du système de contrôle
Risques naturels	Direction de la gestion des risques naturels, ministère de l'Intérieur	Stratégie nationale de gestion des risques de catastrophes naturelles 2020-2030	Gouvernance intégrée, prévention, financement contingent du risque
Stratégique global	Commission spéciale sur le modèle de développement	Rapport général du Nouveau Modèle de Développement (2021)	Intégration de la résilience dans l'ambition nationale à l'horizon 2035
International	OCDE	Recommandation sur la gouvernance des risques majeurs (2014) ; examens 2016, 2018, 2019, 2023	Diffusion normative, évaluation par les pairs, comparabilité internationale

5. Analyse des résultats : portée et limites de l'intégration sur la gouvernance

5.1 Des acquis tangibles en matière de transparence et de discipline budgétaire

Les résultats de cette analyse documentaire conduisent d'abord à reconnaître des acquis tangibles. La trajectoire des trois évaluations PEFA conduites en 2009, 2016 et 2023 témoigne d'une amélioration continue, mesurée par un instrument indépendant et internationalement reconnu, de la performance du système marocain de gestion des finances publiques, avec une majorité d'indicateurs désormais notés parmi les plus élevés de l'échelle d'évaluation et une crédibilité explicitement reconnue de la Cour des comptes⁹¹. De même, dans le champ de la

⁹¹Ministère de l'Économie et des Finances du Royaume du Maroc (2024). *Atelier de dissémination des résultats de l'évaluation PEFA 2023*. Rabat, MEF.

gestion des risques de catastrophes naturelles, les réalisations documentées — montée en puissance d’une direction dédiée, mise en place d’un mécanisme hybride de financement du risque effectivement mobilisé après le séisme d’Al Haouz, déploiement opérationnel d’un système d’alerte précoce — ne relèvent pas du seul affichage stratégique mais traduisent des capacités effectives de résilience institutionnelle. Ces deux champs constituent, au sein du cas marocain, les domaines où l’intégration entre risque et planification stratégique apparaît la plus consolidée et la plus opérationnellement vérifiable.

5.2 Une intégration asymétrique et sectorisée

Cette consolidation contraste cependant avec un constat de sectorisation plus large de l’intégration observée. Les stratégies sectorielles « ordinaires » qui ont marqué les deux dernières décennies de planification marocaine — dans l’agriculture, l’industrie ou le tourisme notamment — ont généralement été construites autour d’objectifs quantitatifs ambitieux, sans que leur conception intègre systématiquement une évaluation ex ante des vulnérabilités susceptibles d’en compromettre la réalisation. Le diagnostic même porté par la Commission spéciale sur le modèle de développement, en identifiant les défaillances du modèle antérieur, peut se lire comme la reconnaissance a posteriori de ce déficit d’anticipation des risques systémiques dans la conception des politiques sectorielles précédentes. Cette asymétrie se double d’une dimension territoriale, mise en évidence par le Conseil économique, social et environnemental à propos de la stratégie de gestion des risques de catastrophes naturelles elle-même : un cadre stratégique national mature peut coexister avec une appropriation inégale à l’échelle régionale et locale, faute d’une diffusion suffisante de l’information et d’une territorialisation effective des outils de connaissance du risque. Le rapport régional de l’OCDE publié en 2019 apporte un éclairage complémentaire à ce constat, en reliant cette difficulté à une tradition administrative centralisée et hiérarchique, organisée en silos ministériels, qui complique structurellement l’appropriation simultanée, par les gestionnaires de terrain, d’une logique de résultats et d’une logique de maîtrise des risques⁹².

5.3 Entre appropriation managériale et isomorphisme institutionnel

La mise en regard de ces constats avec le cadre néo-institutionnaliste mobilisé en section 2.3 invite à formuler une hypothèse interprétative, que les seules sources documentaires rassemblées ne permettent pas de trancher de manière définitive mais qu’elles autorisent à formuler avec prudence. La chronologie même de l’engagement marocain — adhésion à la recommandation de l’OCDE en 2014, revue par les pairs en 2016, diagnostic d’intégrité en 2018, comparaison régionale en 2019, examen global en 2023 — dessine un processus d’internalisation largement scandé par le calendrier des partenaires techniques et financiers internationaux, ce qui correspond assez précisément aux mécanismes d’isomorphisme normatif

⁹²OCDE (2019). *Examens de l’OCDE sur la gouvernance publique : contrôle interne et gestion des risques pour l’intégrité publique au Moyen-Orient et en Afrique du Nord*. Paris, Éditions OCDE.

et mimétique décrits par DiMaggio et Powell (1983)⁹³. Cette observation n'invalide en rien la réalité des progrès enregistrés, en particulier dans les champs budgétaire et des risques naturels où des capacités opérationnelles concrètes ont été documentées ; elle invite cependant à ne pas exclure, dans les champs sectoriels moins exposés au regard international, l'existence d'un certain degré de découplage, au sens de Meyer et Rowan (1977), entre l'adoption de cadres formels de gestion des risques et leur appropriation effective par les gestionnaires de terrain⁹⁴. Cette hypothèse, qui ne peut être confirmée par la seule analyse documentaire mobilisée ici, constitue précisément l'une des pistes de recherche empirique complémentaire identifiées en conclusion.

5.4 Facteurs explicatifs des limites observées

Plusieurs facteurs, convergents à travers les sources mobilisées, contribuent à expliquer les limites ainsi identifiées. Le premier tient à la persistance d'une culture administrative centralisée et hiérarchique, explicitement relevée par l'OCDE comme un obstacle structurel partagé par plusieurs économies de la région⁹⁵. Le second tient à une diffusion encore inégale d'une culture partagée de gestion des risques au-delà des départements ministériels les plus directement concernés — finances, intérieur —, qui disposent de ressources humaines spécialisées et d'une légitimité institutionnelle ancienne, contrairement à de nombreux ministères dits « métiers » dont les capacités internes en matière de gestion des risques demeurent plus limitées. Le troisième tient à la discontinuité propre aux cycles politiques et administratifs, identifiée par la Commission spéciale sur le modèle de développement elle-même comme une caractéristique récurrente de la trajectoire marocaine de planification, qui fragilise la pérennité des dispositifs de suivi des risques au-delà du mandat de leurs initiateurs. Le quatrième, enfin, tient au caractère encore relativement récent — une décennie environ — du processus d'internalisation des standards internationaux de gouvernance du risque, processus dont la maturation, à l'examen même des sources qui le documentent, demeure explicitement présentée comme inachevée par les évaluateurs internationaux eux-mêmes.

6. Discussion

Ces résultats invitent à une discussion en trois temps. Premièrement, ils confirment partiellement, sans la valider intégralement, la thèse du « management du risque généralisé » formulée par Power (2004)⁹⁶ : la prolifération de dispositifs formels — cartographies,

⁹³DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147-160.

⁹⁴Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: formal structure as myth and ceremony. *American Journal of Sociology*, 83(2), 340-363.

⁹⁵OCDE (2019). *Examens de l'OCDE sur la gouvernance publique : contrôle interne et gestion des risques pour l'intégrité publique au Moyen-Orient et en Afrique du Nord*. Paris, Éditions OCDE.

⁹⁶Power, M. (2004). *The Risk Management of Everything: Rethinking the Politics of Uncertainty*. Londres, Demos.

observatoires, chartes — ne se traduit pas mécaniquement par une amélioration substantielle de la décision publique. Le cas marocain montre cependant que cette prolifération peut, dans certaines conditions précises — soutien politique constant, architecture institutionnelle dédiée, financement par des partenariats internationaux durables —, donner lieu à une intégration fonctionnelle réelle, comme en témoignent les cas du pilotage budgétaire et de la gestion des risques de catastrophes naturelles. La portée critique de Power doit donc être nuancée par une lecture davantage centrée sur les mécanismes concrets qui rendent, ou non, possible cette intégration substantielle, plutôt que sur un verdict global et indifférencié.

Deuxièmement, le cas marocain illustre une tension, identifiée en section 2.2 à partir des travaux de Mintzberg (1994)⁹⁷, entre l'héritage d'une tradition de planification rationaliste — héritée des plans de développement successifs — et l'émergence d'une logique plus adaptative, centrée sur la gestion de l'incertitude, que portent à la fois la réforme budgétaire de 2015 et le Nouveau Modèle de Développement de 2021. Cette transition demeure, à l'examen des sources mobilisées, inachevée : le passage d'une planification qui anticipe des résultats à une planification qui anticipe également les risques pesant sur ces résultats ne s'observe pleinement, à ce stade, que dans un nombre restreint de domaines.

Troisièmement, la résilience institutionnelle observée dans le champ des risques naturels apparaît moins comme une propriété générale et diffuse de l'administration marocaine que comme le produit de mécanismes spécifiques et identifiables — une direction dédiée, un financement contingent mobilisable, un système d'alerte opérationnel. Cette lecture, davantage centrée sur des mécanismes circonscrits que sur une qualité structurelle globale, invite à se montrer prudent face à toute généralisation hâtive des progrès observés dans un secteur à l'ensemble de l'appareil administratif marocain. Ces résultats doivent enfin être resitués dans leurs limites de généralisation : ils portent sur un cas unique, à partir de sources essentiellement documentaires, sur une période historique précise — globalement 2014-2024 — et sur des domaines particulièrement exposés au regard international, ce qui invite à la prudence avant toute extrapolation à l'ensemble de l'action publique marocaine ou à d'autres contextes nationaux comparables.

7. Recommandations

Au regard de ces constats, plusieurs recommandations peuvent être formulées à l'attention des différents acteurs concernés. Pour les autorités budgétaires, il paraît souhaitable d'approfondir l'articulation déjà engagée entre les indicateurs des projets de performance et une identification explicite des risques pesant sur l'atteinte de ces objectifs, par exemple en intégrant systématiquement, dans la documentation budgétaire soumise au débat parlementaire, une rubrique consacrée aux principaux risques associés à chaque programme. Pour les ministères sectoriels dits « métiers », la création de points focaux ou de cellules légères de gestion des risques, inspirées du modèle de la Direction de la gestion des risques naturels mais dimensionnées aux moyens de chaque département, permettrait de combler le déficit de

⁹⁷Mintzberg, H. (1994). *The Rise and Fall of Strategic Planning*. New York, Free Press.

capacités internes identifié en section 5.4, à condition que ces cellules soient effectivement reliées au pilotage stratégique des politiques sectorielles et non cantonnées à une fonction de reporting formel.

À l’échelle territoriale, la recommandation déjà formulée par le Conseil économique, social et environnemental⁹⁸ — intégrer les axes de la stratégie nationale de gestion des risques dans les documents de planification régionale et locale — gagnerait à être étendue, au-delà du seul champ des risques naturels, à l’ensemble des dimensions du risque pertinentes pour les territoires, ce qui suppose un effort conséquent de formation des cadres territoriaux et de mise à disposition des données produites par l’Observatoire national des risques naturels. Pour la fonction de contrôle et d’audit, l’extension de l’approche d’audit fondé sur les risques, aujourd’hui principalement portée par l’Inspection générale des finances, à un réseau plus large de structures d’inspection ministérielle, sur la base d’une méthodologie harmonisée de cartographie des risques, permettrait de diffuser plus largement une culture commune du contrôle par les risques. Plus largement, un effort soutenu de formation continue des cadres administratifs aux méthodologies de gestion des risques, au-delà des seuls départements historiquement les plus avancés en la matière, apparaît nécessaire pour desserrer la contrainte que représente, selon le diagnostic régional de l’OCDE, la tradition administrative centralisée et hiérarchique. Enfin, l’institutionnalisation d’un mécanisme national et périodique d’évaluation de la qualité de l’anticipation des risques dans les stratégies sectorielles, indépendant du seul calendrier des évaluations internationales, permettrait d’ancrer cette préoccupation dans une dynamique de pilotage endogène plutôt que dans une dépendance exclusive aux échéances fixées par les partenaires techniques et financiers.

Tableau 2. Synthèse des recommandations

Recommandation	Acteur principal concerné	Horizon
Intégrer une rubrique « risques » dans les projets de performance soumis au Parlement	Direction du Budget, ministères sectoriels	Court terme
Créer des cellules légères de gestion des risques dans les ministères « métiers »	Ministères sectoriels	Moyen terme
Territorialiser les outils nationaux de connaissance du risque	Collectivités territoriales, Observatoire national des risques naturels	Moyen terme
Étendre l’audit fondé sur les risques à un réseau élargi d’inspections ministérielles	Inspection générale des finances, inspections sectorielles	Moyen terme

⁹⁸Conseil économique, social et environnemental [CESE] (2024). *Pour une gestion efficace et proactive des risques des catastrophes naturelles : rôles et capacités des acteurs territoriaux*. Rabat, CESE.

Renforcer la formation continue à la gestion des risques	Instituts de formation de l'administration publique	Long terme
Instituer une évaluation nationale périodique et indépendante de l'anticipation des risques	Conseil économique, social et environnemental, ou instance ad hoc	Long terme

8. Conclusion et perspectives de recherche

Cet article s'est proposé d'examiner comment la gestion des risques s'intègre dans la planification stratégique publique marocaine et quels effets cette intégration produit sur la gouvernance. L'analyse documentaire conduite met en évidence une intégration réelle mais asymétrique : fermement institutionnalisée dans le champ budgétaire, où elle s'adosse à la réforme de la loi organique relative à la loi de finances et se traduit par des progrès mesurés et indépendamment vérifiés, et dans le champ de la gestion des risques de catastrophes naturelles, où elle a donné lieu à des capacités opérationnelles concrètes ; affirmée avec ambition au plus haut niveau stratégique par le Nouveau Modèle de Développement, qui érige désormais la résilience en finalité explicite de l'action publique ; mais nettement moins consolidée au sein de la planification stratégique sectorielle ordinaire et à l'échelle territoriale, où des logiques de conformité formelle semblent encore prévaloir sur une appropriation managériale pleinement assumée. Les effets de cette intégration sur la gouvernance apparaissent, en conséquence, eux-mêmes différenciés : tangibles et mesurables dans certains champs, plus incertains et potentiellement performatifs dans d'autres.

Cette recherche contribue à une littérature encore relativement peu développée sur l'articulation entre gestion des risques et planification stratégique dans des contextes d'économie émergente situés hors du cœur historique de l'OCDE, en proposant une grille d'analyse à trois dimensions — cadres, mécanismes, effets — susceptible d'être reproduite dans d'autres contextes nationaux comparables. Elle invite, dans le même mouvement, à plusieurs prolongements. Une première perspective consisterait à compléter cette analyse documentaire par une enquête de terrain — entretiens auprès de gestionnaires de risques sectoriels, de cadres territoriaux et de parlementaires impliqués dans l'examen des projets de performance — afin de tester empiriquement l'hypothèse de découplage formulée en section 5.3. Une seconde perspective gagnerait à inscrire le cas marocain dans une comparaison régionale, notamment avec d'autres économies du Moyen-Orient et d'Afrique du Nord engagées dans des trajectoires de réforme similaires sous l'égide de l'OCDE, afin de déterminer si les facteurs explicatifs identifiés en section 5.4 relèvent d'une spécificité nationale ou d'une dynamique régionale plus large. Une troisième perspective consisterait à approfondir, par des études de cas sectorielles dédiées — la gestion du système de santé après la pandémie, ou la gestion de la ressource en eau face à l'accélération du stress hydrique —, la possibilité de répliquer la logique observée dans le champ des risques naturels à d'autres secteurs exposés à des risques systémiques comparables. Une quatrième perspective, de nature plus quantitative, consisterait à construire un indice composite de maturité de la gestion des risques applicable aux différentes stratégies sectorielles

marocaines, permettant des comparaisons longitudinales et inter-ministérielles que la présente démarche qualitative ne permet pas, par construction, d'établir. Une dernière perspective, enfin, gagnerait à explorer plus spécifiquement l'échelle territoriale, afin de mieux comprendre les conditions dans lesquelles les régions et les communes marocaines s'approprient, ou au contraire peinent à s'approprier, les cadres nationaux de gestion des risques, prolongeant ainsi directement le constat de fragmentation centre-périphérie mis en évidence dans cette recherche.

Références bibliographiques

- Banque mondiale (2024). *Des catastrophes aux opportunités : construire un avenir résilient au Maroc*. Washington, World Bank Group.
- Bardin, L. (1977). *L'analyse de contenu*. Paris, Presses universitaires de France.
- Beck, U. (2001 [1986]). *La société du risque : sur la voie d'une autre modernité*. Paris, Aubier.
- Bensouda, N. (2012). *La réforme de la loi organique des finances : vers un nouveau modèle de gestion des finances publiques*. Communication, Association des membres de l'Inspection générale des finances, Rabat.
- Commission spéciale sur le modèle de développement [CSMD] (2021). *Le Nouveau Modèle de Développement : libérer les énergies et restaurer la confiance pour accélérer la marche vers le progrès et la prospérité pour tous — Rapport général*. Rabat, CSMD.
- Conseil économique, social et environnemental [CESE] (2024). *Pour une gestion efficace et proactive des risques des catastrophes naturelles : rôles et capacités des acteurs territoriaux*. Rabat, CESE.
- Committee of Sponsoring Organizations of the Treadway Commission [COSO] (2017). *Enterprise Risk Management — Integrating with Strategy and Performance*. New York, COSO.
- DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147-160.
- Douglas, M., & Wildavsky, A. (1982). *Risk and Culture: An Essay on the Selection of Technological and Environmental Dangers*. Berkeley, University of California Press.
- Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. Dans N. K. Denzin & Y. S. Lincoln (dir.), *Handbook of Qualitative Research* (p. 105-117). Thousand Oaks, Sage.
- Hood, C. (1991). A public management for all seasons? *Public Administration*, 69(1), 3-19.
- International Organization for Standardization [ISO] (2018). *ISO 31000:2018 — Management du risque : lignes directrices*. Genève, ISO.
- Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: formal structure as myth and ceremony. *American Journal of Sociology*, 83(2), 340-363.
- Ministère de l'Économie et des Finances du Royaume du Maroc (2024). *Atelier de dissémination des résultats de l'évaluation PEFA 2023*. Rabat, MEF.
- Mintzberg, H. (1994). *The Rise and Fall of Strategic Planning*. New York, Free Press.

- Organisation de coopération et de développement économiques [OCDE] (2014). *Recommandation du Conseil sur la gouvernance des risques majeurs*. Paris, OCDE.
- OCDE (2016). *L'étude de l'OCDE sur la gestion des risques au Maroc*. Paris, Éditions OCDE.
- OCDE (2018). *Examens de l'OCDE sur la gouvernance publique : diagnostic d'intégrité au Maroc*. Paris, Éditions OCDE.
- OCDE (2019). *Examens de l'OCDE sur la gouvernance publique : contrôle interne et gestion des risques pour l'intégrité publique au Moyen-Orient et en Afrique du Nord*. Paris, Éditions OCDE.
- OCDE (2023). *Examens de l'OCDE sur la gouvernance publique : Maroc — pour une administration résiliente au service des citoyens*. Paris, Éditions OCDE.
- Power, M. (2004). *The Risk Management of Everything: Rethinking the Politics of Uncertainty*. Londres, Demos.
- Renn, O. (2008). *Risk Governance: Coping with Uncertainty in a Complex World*. Londres, Earthscan.
- Royaume du Maroc (2015a). *Loi organique n° 130-13 relative à la loi de finances*, promulguée par le dahir n° 1-15-62 du 2 juin 2015, Bulletin officiel n° 3107.
- Royaume du Maroc (2015b). *Décret n° 2-15-426 du 15 juillet 2015 relatif à l'élaboration et à l'exécution des lois de finances*.
- Royaume du Maroc, ministère de l'Intérieur (2020). *Stratégie nationale de gestion des risques des catastrophes naturelles 2020-2030*. Rabat.
- Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods* (6e éd.). Thousand Oaks, Sage.

CHAPITRE 09: *IA générative, automatisation marketing et risques numériques : une approche Design Science Research*

Leila BAKHTI

Laboratoire MADEO, EST Oujda. bakhtileila90@gmail.com

Ibtissam ARRASSEN,

Laboratoire LARI, FS Oujda. i.arrassen@ump.ac.ma

Mohammed ERRAMDANI,

Laboratoire MADEO, EST Oujda. m.erramdani@ump.ac.ma

L'automatisation du marketing digital connaît une évolution rapide sous l'effet de l'IA générative et, en particulier, des modèles LLM. Les organisations ne se limitent plus à utiliser des outils d'automatisation pour optimiser des campagnes ; elles explorent désormais la capacité des LLM à transformer des représentations organisationnelles en artefacts numériques directement exploitables. Cette évolution modifie la manière dont les funnels marketing sont conçus, structurés et déployés dans les systèmes d'information des entreprises.

Le développement de l'automatisation du marketing digital repose aujourd'hui sur l'orchestration du parcours client et l'exécution automatisée des interactions. Le funnel marketing constitue l'architecture opérationnelle centrale de cette automatisation. Il organise les étapes du parcours, relie contenus et métriques et structure la progression du prospect vers la conversion. L'IA agit comme un moteur transversal d'optimisation, capable d'améliorer la performance et la cohérence des actions marketing.

Les LLM introduisent une capacité supplémentaire : transformer des schémas métiers en outputs numériques concrets, tels que des pages web structurées en HTML et CSS. Ils jouent un rôle de médiation entre la logique marketing et l'implémentation technique. Cette capacité ouvre des perspectives nouvelles pour la conception d'artefacts numériques.

Toutefois, cette transformation soulève des enjeux importants. La fiabilité des contenus générés, la gouvernance des données, la cybersécurité et la responsabilité organisationnelle deviennent des dimensions centrales. Les modèles peuvent produire des contenus plausibles mais inexacts, intégrer des biais ou générer des structures qui s'éloignent de la logique métier initiale.

Au-delà des aspects techniques, l'intégration des LLM implique des transformations organisationnelles. Les rôles évoluent, les compétences doivent être adaptées et les mécanismes de coordination doivent être repensés. La réussite de cette transition dépend d'un management de changement structuré, capable d'articuler innovation technologique, contrôle des risques et gouvernance réfléchie.

Dans ce contexte, la littérature traite encore insuffisamment les mécanismes de transformation reliant des représentations métier orientées funnels marketing à des artefacts numériques exploitables dans des systèmes d'information. Cette limite met en évidence une problématique centrale portant sur la capacité des modèles LLM à assurer une médiation cohérente entre logique métier, structuration des workflows marketing et implémentation numérique, tout en intégrant les enjeux liés aux risques numériques, à la gouvernance et au management du changement. Dès lors, cette recherche s'interroge sur la question suivante : Comment un modèle

LLM peut-il être mobilisé comme mécanisme de transformation entre des représentations métier orientées funnels marketing et des artefacts numériques exploitables dans une logique de système d'information, tout en prenant en compte les risques numériques, la gouvernance des données et les enjeux de conduite du changement organisationnel ? Dans cette perspective, l'étude adopte une approche de type Design Science Research afin d'analyser la formalisation de funnels marketing orientés métier ainsi que les transformations numériques produites par les LLM, tout en discutant les conditions organisationnelles nécessaires à une automatisation responsable et maîtrisée.

Cet article est structuré comme suit. La section 2 présente la revue de la littérature et le cadre théorique mobilisé autour de l'automatisation du marketing digital, des modèles LLM, des risques numériques et du management du changement. La section 3 expose la méthodologie de recherche fondée sur le Design Science Research ainsi que la formalisation des funnels marketing mobilisés dans cette étude. La section 4 présente les résultats obtenus à partir des transformations réalisées par le LLM et développe une discussion critique portant sur les mécanismes de transformation observés, les limites de l'approche proposée, les risques liés aux LLM ainsi que les enjeux organisationnels associés au management du changement. Enfin, la section 5 revient sur les principales contributions théoriques, méthodologiques et managériales de la recherche, tout en présentant les limites de l'étude et les perspectives futures.

1. Revue de la littérature et cadre théorique

1.1 Revue de la littérature

Concernant l'automatisation du marketing digital, de nombreux travaux académiques ont progressivement éclairé les pratiques associées à son déploiement dans les organisations. Nous nous appuyons ici sur quelques articles de référence afin d'en présenter les principaux apports. Mero et al. (2022) montrent comment une logique agile permet d'intégrer progressivement l'automatisation dans les processus marketing. La contribution principale réside dans l'explication du passage d'un marketing manuel vers un marketing automatisé. Guercini (2023) examine comment les outils de marketing automatisé influencent les décisions des responsables marketing. Pour Saura et al. (2021), la contribution principale de cet article est de relier marketing automatisé et IA dans une perspective B2B structurée. Silva et al. (2023) ont montré que la valeur ajoutée réside dans l'approche managériale du marketing automatisé comme outil de pilotage stratégique. Kshetri et al. (2024) présentent un cadre clair sur ce que l'IA générative apporte au niveau des processus marketing orienté données. Grewal et al. (2025) expliquent comment les LLM transforment l'exécution marketing, et comment cela accélère

l'automatisation. Cillo et al. (2025) proposent une feuille de route sur l'intégration de l'IA générative dans les processus marketing.

Concernant les LLM et leur rôle dans la transformation des artefacts marketing en applications utiles pour l'entreprise, la littérature récente souligne leur capacité à convertir des modèles marketing en solutions numériques opérationnelles. Dans ce sens, Feuerriegel et al. (2024) présentent une synthèse académique sur les modèles génératifs et leur intégration dans les systèmes d'information. Bilgihan et al. (2024) proposent un modèle conceptuel intégrant l'IA générative dans les différentes étapes du marketing digital. Schweidel et al. (2024) analysent le rôle croissant des LLM dans l'évolution des pratiques marketing digitales. Estevez et al. (2025) examinent le rôle des LLM dans l'évolution des pratiques de recherche marketing. Les auteurs de cet article montrent que les LLM ne se limite pas à la création de contenu, mais facilite l'exploitation stratégique des données marketing.

Concernant les enjeux de sécurité et les aspects organisationnels liés à l'utilisation des LLM, la littérature met en avant la nécessité d'un encadrement fondé sur la gouvernance des données, la gestion des risques et la responsabilité managériale. Dans ce sens, Miles et al. (2025) proposent une cartographie structurée des risques de sécurité propres aux LLM. Ferrag et al. (2025) relient explicitement les usages cybersécurité des LLM et leurs vulnérabilités et les implications opérationnelles. Gavin et al. (2025) étudient l'usage des LLM dans la gestion d'incidents et met en évidence les limites critiques pour un usage sécurisé. Dwivedi et al. (2023) analysent les implications organisationnelles de l'usage des LLM dans les entreprises. Taeihagh (2025) examine les défis organisationnels associés à la gouvernance des LLM. Kanbach et al. (2024) examinent l'émergence des LLM comme un moteur de transformation des pratiques organisationnelles et décisionnelles.

2.2 Cadre théorique et concepts mobilisés

2.2.1 Automatisation du marketing digital

L'automatisation du marketing digital est comprise comme une capacité organisationnelle permettant de coordonner contenus numériques et plateformes technologiques afin de piloter les interactions digitales et améliorer la performance marketing (Mero et al., (2022)). Shankar et al. (2022) montrent que cette automatisation repose sur la traçabilité des interactions et l'optimisation continue des communications numériques. Les travaux récents sur l'IA en marketing soulignent que ces capacités reposent de plus en plus sur la personnalisation algorithmique et l'orchestration du parcours client numérique (Kumar et al. (2024)).

Dans la littérature récente sur les méthodes d'automatisation du marketing digital, plusieurs travaux académiques convergent vers trois approches devenues particulièrement structurantes avec l'essor de l'IA. Ensemble, ces méthodes montrent que l'IA s'impose progressivement comme un levier central pour soutenir une automatisation plus efficace et mieux orientée vers la décision managériale :

1. Orchestration intelligente du funnel marketing et du parcours digital :

La première méthode structurante consiste à articuler l'orchestration des éléments autour du funnel digital, qui agit aujourd'hui comme l'architecture opérationnelle principale de l'automatisation. Les travaux récents montrent que l'alignement des contenus sur les phases du parcours améliore significativement l'engagement et permet une vraie automatisation pilotable (Weidig et al., 2024 ; Salonen et al., 2024 ; Colicev et al., 2019 ; Peggiani et Lamberti, 2026).

2. Personnalisation algorithmique et optimisation IA de l'expérience digitale :

La deuxième méthode repose sur la personnalisation algorithmique, qui transforme les données comportementales en adaptations tout au long du funnel. L'IA permet ici d'ajuster les recommandations et d'optimiser les interactions en fonction des signaux d'engagement. Cette approche dépasse la simple segmentation traditionnelle en introduisant une logique d'apprentissage continu orientée conversion et expérience client. La littérature souligne que la personnalisation constitue aujourd'hui le cœur opérationnel de l'automatisation du marketing digital, car elle relie directement donnée, engagement et performance (Bleier et al., 2019 ; Weidig et al., 2024).

3. Programmatique et agents conversationnels :

La troisième méthode regroupe les dispositifs où l'exécution marketing est directement déléguée à des mécanismes algorithmiques et les agents conversationnels. Dans une logique de funnel piloté par l'IA, ces technologies permettent d'automatiser l'acquisition, la qualification et certaines séquences relationnelles tout en optimisant les campagnes. Les recherches récentes insistent toutefois sur les enjeux de confiance et de gouvernance des données associés, qui deviennent des dimensions structurantes de l'automatisation (Palos-Sanchez et al., 2019 ; Thomaz et al., 2020).

Ces méthodes convergent vers une logique commune : le funnel marketing constitue la composante managériale privilégiée, tandis que l'IA agit comme moteur d'optimisation

transversal. Cette intégration explique pourquoi la littérature récente ne traite plus ces pratiques comme des outils isolés, mais comme un système cohérent d'automatisation piloté par l'IA.

2.2.2 Modèles de langage (LLM) et enjeux liés aux risques numériques et management de changement

Les modèles LLM désignent une nouvelle génération de systèmes IA capables de produire des contenus textuels à partir d'un apprentissage à très grande échelle. Brown et al. (2020) montrent que ces modèles peuvent réaliser différentes tâches sans entraînement spécifique, ce qui marque une rupture dans la manière dont les organisations envisagent l'IA appliquée aux activités numériques. Dans une perspective plus synthétique, Kumar (2024) souligne que les LLM constituent désormais une infrastructure technologique majeure pour la transformation digitale.

L'intégration des LLM dans des projets de transformation numérique, notamment lorsqu'il s'agit de convertir des artefacts issus d'un funnel marketing vers des plateformes digitales, soulève toutefois des risques numériques spécifiques. Bender et al. (2021) montrent que les modèles linguistiques peuvent produire des contenus très utiles mais inexacts, ce qui peut fragiliser des processus automatisés s'appuyant sur ces sorties textuelles. Weidinger et al. (2022) identifient différentes catégories de risques incluant la manipulation informationnelle. Dwivedi et al. (2023) soulignent que l'IA générative transforme profondément les pratiques managériales et introduit des défis liés à la responsabilité et à la gouvernance.

Dans les contextes actuels de transformation digitale, notamment dans les économies émergentes où les organisations intègrent progressivement les technologies IA dans leurs systèmes d'information (et leurs pratiques de marketing digital), les enjeux liés aux LLM prennent une dimension particulièrement structurante. Dans le contexte marocain, cette dynamique s'inscrit dans plusieurs initiatives nationales de transformation numérique, notamment la stratégie « Maroc Digital 2030 », portée par le Ministère de la Transition Numérique et de la Réforme de l'Administration, qui vise à renforcer la digitalisation des organisations, le développement des infrastructures numériques, l'intégration de l'intelligence artificielle et l'accompagnement des capacités numériques organisationnelles. Dans ce cadre, les questions liées à la gouvernance des données, à la maturité numérique, à l'appropriation organisationnelle des technologies avancées et à la capacité des équipes à intégrer des mécanismes automatisés dans les processus des entreprises et dans les services de l'administration publique deviennent des facteurs déterminants dans la réussite des projets fondés sur les IA.

Face à ces enjeux, la mise en œuvre de projets intégrant des LLM nécessite un management de changement structuré. L'introduction de ces technologies implique des transformations organisationnelles qui dépassent la seule dimension technique. Kotter (1995) souligne que les initiatives de transformation réussies reposent sur une vision partagée et une mobilisation progressive des acteurs. Ce même auteur souligne, récemment, que ces éléments sont essentiels lorsque les processus marketing sont automatisés par l'IA. Dans le domaine de la transformation digitale, Vial (2019) montre que l'intégration de technologies avancées exige une reconfiguration des capacités organisationnelles et une adaptation des modes de coordination. Enfin, Verhoef et al. (2021) insistent sur le rôle du leadership et de la gouvernance dans la réussite des projets numériques.

Les travaux mobilisés sur l'automatisation du marketing digital, les modèles LLM, les risques numériques et le management du changement permettent de dépasser une lecture strictement descriptive des technologies d'IA générative pour construire une logique conceptuelle intégratrice centrée sur la transformation d'artefacts métier orientés funnels marketing. Dans ce cadre, le funnel marketing est appréhendé comme une représentation métier structurante du parcours digital, tandis que le LLM est conceptualisé comme un mécanisme de médiation et de transformation reliant logique métier et implémentation numérique. Cette transformation conduit à la génération d'artefacts numériques opérationnels pouvant être intégrés dans des systèmes d'information orientés digital marketing. Parallèlement, les dimensions liées à la gouvernance, à la sécurité des données, à la traçabilité et au management du changement constituent des mécanismes organisationnels encadrant l'intégration et l'appropriation de ces transformations numériques. La Figure Fig. 1 formalise cette articulation théorique et met en évidence les relations conceptuelles structurant le cadre proposé.

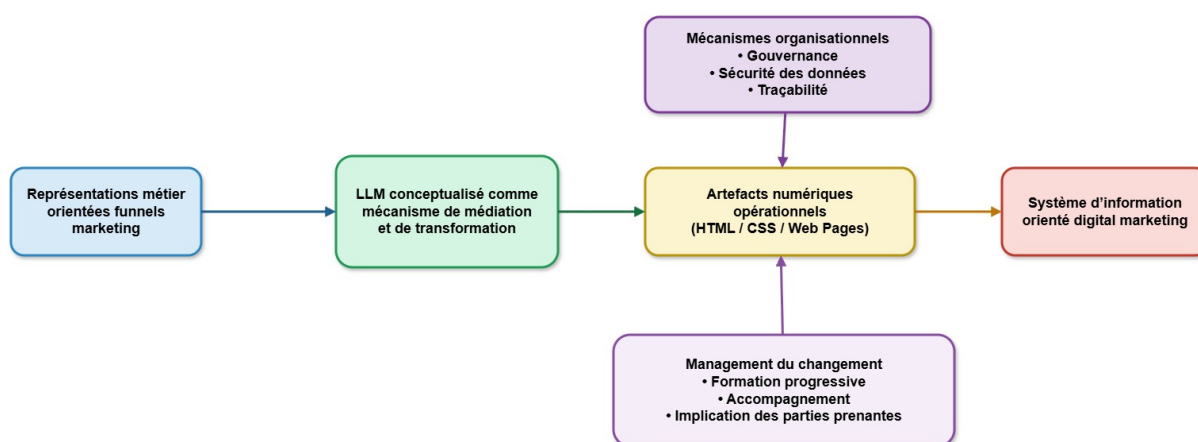


Figure 1 : Cadre conceptuel DSR de transformation des funnels marketing par les LLM

Le cadre conceptuel proposé conduit à formaliser deux propositions conceptuelles structurant la logique théorique de la recherche :

Proposition conceptuelle 1 : Les modèles LLM peuvent être mobilisés comme mécanismes de médiation permettant de transformer des représentations métier orientées funnels marketing en artefacts numériques opérationnels intégrables dans des systèmes d'information orientés digital marketing.

Proposition conceptuelle 2 : L'intégration organisationnelle des artefacts générés par les LLM nécessite des mécanismes complémentaires liés à la gouvernance des données, à la sécurité de l'information et au management du changement afin de garantir la cohérence et l'appropriation des transformations numériques produites.

2. Méthodologie de recherche

3.1 Approche Design Science Research et positionnement épistémologique

Cet article s'inscrit dans une démarche de Design Science Research (DSR) mobilisée dans le champ des sciences de gestion des systèmes d'information. L'objectif n'est pas d'analyser le funnel marketing selon une logique descriptive ou explicative, mais de concevoir des artefacts conceptuels capables de structurer une problématique organisationnelle afin de la traduire dans un système d'information. Dans cette perspective, le funnel marketing digital est abordé comme une représentation métier à formaliser, plutôt que comme un simple objet d'observation empirique. Cette orientation s'inscrit dans la tradition du DSR où la production d'artefacts constitue une contribution scientifique centrale orientée vers la résolution de problèmes de conception (Hevner et al., 2004 ; March & Smith, 1995).

Le DSR est ici adopté, donc, dans une posture constructiviste, où la connaissance émerge progressivement à travers la conception d'objets intermédiaires servant à comprendre une réalité organisationnelle. Les artefacts proposés constituent avant tout des supports d'analyse permettant de voir comment une représentation métier (en l'occurrence le funnel marketing digital) peut être traduite dans une structure de système d'information. Cette logique rejoint la vision des sciences de l'artificiel où la conception joue un rôle central dans la production de connaissances actionnables (Simon, 1996 ; van Aken, 2004).

Dans ce cadre, l'approche proposée repose sur la conception d'un funnel marketing orienté métier, associé à des règles de transformation mobilisant un modèle de langage de type LLM. L'enjeu n'est pas la performance technique du modèle, mais la médiation qu'il permet entre

logique organisationnelle et logique applicative. Le processus de transformation devient ainsi un objet d'analyse en soi, dans une perspective de « design knowledge » telle que discutée dans les travaux pertinents en DSR (Gregor & Hevner, 2013 ; Baskerville et al., 2018).

Conformément aux principes de la DSR, la recherche suit une logique de conception, de démonstration et d'évaluation de l'artefact. La phase de conception formalise le funnel selon une logique de processus inspirée des pratiques de modélisation organisationnelle. Les diagrammes produits adoptent une structuration séquentielle proche de certaines représentations BPMN (Business Process Management Notation) dans la mesure où ils organisent des étapes, des transitions et des flux d'action. Toutefois, il ne s'agit pas d'une modélisation BPMN formelle mais d'une représentation simplifiée orientée métier, dont l'objectif est de faciliter la compréhension et la transformation conceptuelle vers une architecture de système d'information, conformément aux recommandations méthodologiques du DSR qui privilégient la pertinence et l'utilité de l'artefact dans son contexte d'usage (Peffer et al., 2007 ; Iivari, 2015).

3.2 Formalisation des funnels marketing à l'aide du DSR

La démarche s'appuie sur les étapes du DSR proposées par Peffer et al. (2007). Afin de rendre explicite l'opérationnalisation de cette démarche dans cette recherche, le Tableau Tab. 1 synthétise les différentes étapes méthodologiques mobilisées ainsi que leur traduction concrète dans le processus de conception, de transformation et d'évaluation des artefacts proposés.

Tableau 1 : Opérationnalisation de la démarche DSR

Étapes DSR (Peffer et al., 2007)	Objectif méthodologique	Mise en œuvre dans cette recherche
Identification du problème	Identifier les limites des approches actuelles de transformation des funnels marketing	Analyse des limites de transformation des représentations métier vers des artefacts numériques exploitables
Définition des objectifs	Définir une logique de transformation orientée SI	Formalisation d'un mécanisme de médiation fondé sur les LLM
Conception et développement	Construire les artefacts et règles de transformation	Conception des funnels marketing et structuration des règles de transformation

Démonstration	Montrer la faisabilité de la transformation	Génération d'artefacts numériques HTML/CSS à partir des funnels
Évaluation	Examiner la cohérence des transformations produites	Analyse de la préservation des étapes métier et des transitions.
Communication	Formaliser et diffuser les connaissances produites	Production du cadre conceptuel et des résultats de cette recherche

3.2.1 La phase de conception et de développement des artefacts

Le funnel marketing est une séquence d'étapes qui relie les différents leviers numériques aux niveaux d'engagement des clients. Chaque segment du funnel correspond à un objectif spécifique et sert de cadre pour mesurer l'effet des actions numériques sur l'engagement (Madhushan et al. 2024). La littérature montre que le funnel marketing ne se limite pas à une seule configuration, mais qu'il existe plusieurs formes adaptées aux objectifs et aux contextes digitaux (Court et al., 2009 ; Kotler & Keller, 2016). Afin d'ancrer la démarche DSR dans des pratiques réelles du marketing digital, la recherche mobilise trois types de funnels largement utilisés dans les stratégies numériques contemporaines à l'échelle internationale : le lead funnel, le funnel de vente et le webinar funnel. Ces configurations, aujourd'hui fortement présentes dans les pratiques terrain d'automatisation marketing, sont mobilisées comme cas expérimentaux permettant d'observer la capacité des modèles LLM à transformer des représentations métier orientées marketing en artefacts numériques opérationnels intégrables dans des systèmes d'information orientés digital marketing. Le choix de ces cas repose sur leur rôle structurant dans les logiques d'acquisition, d'engagement et de conversion mobilisées dans les parcours digitaux contemporains :

- Le funnel orienté Vente (Fig. 2) : Ce funnel est utilisé comme cadre analytique central pour mesurer l'impact différencié des actions marketing sur la progression du consommateur vers l'achat (Colicev et al. 2018).

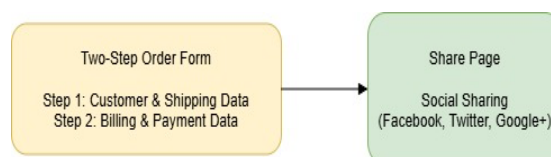


Figure 2 : Exemple de funnel de vente

- Lead Generation Funnel : Fig. 3 illustre un lead funnel simplifié structurant la progression d'un internaute vers une action. La figure 3 commence par une page de

capture conçue pour recueillir l'adresse email du visiteur à l'aide d'un titre accrocheur et d'un bouton d'action simple. Après cette étape, l'utilisateur est dirigé vers une page de remerciement intégrant une vidéo, qui permet de maintenir son attention et de renforcer l'intérêt pour l'offre. En arrière-plan, une séquence d'emails automatisée se déclenche afin d'accompagner progressivement le prospect.

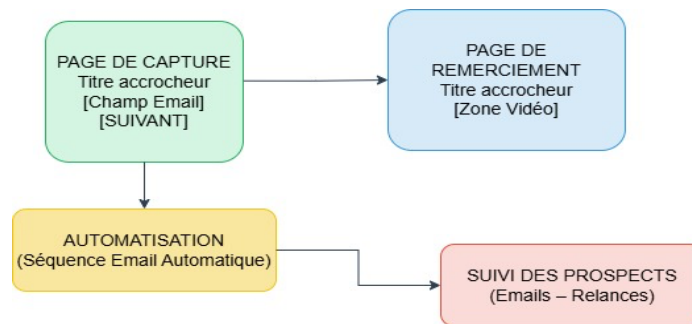


Figure 3 : Exemple de lead funnel

- Webinar Funnel : La figure 4 commence par une page d'inscription au webinar, pensée pour inciter rapidement le visiteur à laisser son email grâce à un message clair et un bouton d'inscription direct. Une fois inscrit, l'utilisateur arrive sur une page de confirmation qui lui propose d'ajouter le rendez-vous à son calendrier, ce qui facilite sa participation.

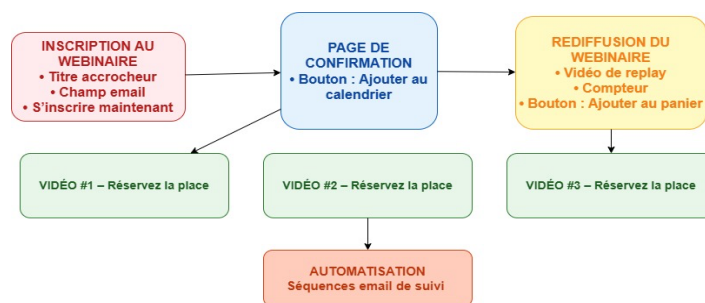


Figure 4 : Exemple de funnel Webinar

3.2.2 La phase de démonstration et d'évaluation

Dans cet article, la phase de démonstration repose sur l'utilisation d'un LLM comme mécanisme de transformation des artefacts conçus. La démonstration consiste ainsi à illustrer le passage d'une représentation marketing initiale vers des structures informationnelles opérationnelles, en mettant l'accent sur le rôle médiateur du LLM dans ce processus de

transformation. Cette approche permet de rendre visible la valeur de l’artefact, en montrant sa capacité à soutenir une logique de conception orientée usage organisationnel, conformément à la phase de démonstration du DSR (Peffer et al., 2007). Dans ce sens, la figure 5 met surtout en évidence un processus de transformation. Le « vibe coding » et les artefacts issus des funnels (Fig. 2, Fig.3 et Fig.4) constituent les deux points d’entrée du système. Le LLM intervient sur ces éléments qui sont interprétés et traduits sous une forme exploitable.

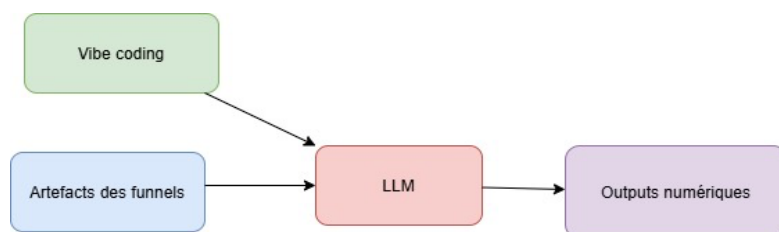


Figure 5 : Transformation des artefacts de funnels par un LLM vers des outputs numériques

Afin de rendre plus explicite la dimension empirique de la démarche DSR, le tableau Tab. 2 suivant synthétise les principaux artefacts mobilisés, les exemples de vibe coding transmis au LLM ainsi que les outputs numériques générés et les observations analytiques associées.

Tableau 2 : Structuration empirique des transformations d’artefacts de funnels par le LLM

Type de funnel mobilisé	Nature de l’artefact métier	Exemple de vibe coding / instruction transmise au LLM	Output numérique généré	Observations analytiques
Lead Funnel	Structure de capture de prospects avec automatisation email progressive	« Génère une landing page HTML/CSS simple permettant la capture d’email avec un bouton Call-To-Action et une transition vers une page de remerciement intégrant une vidéo. »	Landing page HTML/CSS + page de remerciement + structure d’automatisation	La logique de capture et de transition reste cohérente avec le parcours métier initial.

Webinar Funnel	Processus d'inscription et de confirmation à un webinaire	« Génère une page webinar HTML/CSS contenant un formulaire d'inscription, un bouton d'ajout calendrier et une page de confirmation structurée. »	Page webinar opérationnelle HTML/CSS + page confirmation	Le LLM préserve la logique séquentielle du funnel et produit une structure numérique cohérente.
Funnel de vente	Parcours orienté conversion et passage à l'achat	« Génère une page de vente HTML/CSS contenant présentation produit, bouton d'achat, formulaire de paiement et page de validation de commande. »	Sales page HTML/CSS + checkout page + confirmation page	Les transitions entre les étapes commerciales demeurent structurées et intégrables dans une architecture SI.
Funnel orienté partage social	Workflow de diffusion et de partage d'offre	« Génère une page HTML/CSS intégrant des boutons de partage social et une logique d'incitation au partage après inscription. »	Social sharing page HTML/CSS	Le LLM conserve les relations fonctionnelles entre engagement utilisateur et diffusion numérique.
Funnel multi-étapes	Workflow marketing séquentiel avec navigation progressive	« Génère un funnel multi-step HTML/CSS avec indicateur d'étapes, navigation conditionnelle et validation progressive des informations utilisateur. »	Multi-step funnel HTML/CSS	Les étapes et transitions restent observables et cohérentes dans une perspective de transformation SI.

Dans la phase d'évaluation, l'analyse porte sur la cohérence des transformations produites par le LLM à partir des représentations métier initiales. L'évaluation s'appuie sur plusieurs

dimensions analytiques liées à la préservation de la structure du funnel, à la cohérence des transitions entre les étapes et à l'exploitabilité des artefacts numériques générés dans une logique de système d'information orienté digital marketing. Ces dimensions d'analyse sont synthétisées dans le Tableau Tab. 3 et seront mobilisées afin d'examiner les outputs produits par le LLM.

Tableau 3 : Procédures d'analyse appliquées au webinar funnel

Dimensions d'analyse	Description analytique appliquée au webinar funnel	Objectif analytique
Conservation des étapes du webinar funnel	Vérification de la présence des différentes étapes du webinar funnel dans les pages générées par le LLM : page de présentation du webinar, formulaire d'inscription, bouton « S'inscrire », page de confirmation et ajout au calendrier.	Vérifier que le LLM conserve correctement la structure métier initiale du webinar funnel.
Analyse des transitions entre les pages	Observation du passage entre les différentes pages générées, par exemple entre le clic sur le bouton d'inscription, l'envoi du formulaire et l'affichage de la page de confirmation.	Vérifier la cohérence du parcours utilisateur et la continuité logique des transitions générées.
Analyse des formulaires et boutons d'action	Vérification de la présence et du fonctionnement des formulaires de capture d'email, des boutons d'appel à l'action et des mécanismes d'inscription au webinar.	Examiner la capacité du LLM à reproduire les principaux mécanismes d'interaction utilisés dans les webinar funnels réels.
Analyse de la structure HTML/CSS générée	Observation de l'organisation des sections HTML/CSS produites : blocs de contenu, formulaires, boutons, titres, zones de présentation du webinar et sections de confirmation.	Évaluer la stabilité technique et la lisibilité des artefacts numériques générés par le LLM.
Analyse des mécanismes d'engagement	Vérification de la présence des éléments destinés à maintenir l'engagement du visiteur : message de confirmation, rappel du	Examiner si les mécanismes d'engagement du webinar funnel sont conservés dans les outputs générés.

	webinar, ajout au calendrier et éléments d'incitation à participer.	
Analyse de l'intégration SI	Observation de la capacité des pages générées à être intégrées dans un système d'information orienté digital marketing : automatisation des inscriptions, suivi des participants et gestion des interactions.	Évaluer l'exploitabilité des outputs générés dans une logique de système d'information.
Analyse de la cohérence métier globale	Vérification de la correspondance entre les objectifs initiaux du webinar funnel et les pages effectivement produites par le LLM.	Vérifier que la logique métier du webinar funnel reste cohérente après transformation par le LLM.

3. Résultats et discussion critique : limites, risques des LLM et management de changement

4.1 Résultat

Les expérimentations ont été réalisées sur la configuration suivante :

- Environnement matériel : Processeur : 12th Gen Intel® Core™ i7-12700H, Mémoire vive (RAM) : 16 Go et Stockage : SSD 1 To
- Environnement logiciel : Système d'exploitation : Windows 11 (64 bits) et Langages de développement web utilisé par le LLM : HTML et CSS
- Modèle de langage : ChatGPT-5.0, mode déterministe

Les résultats (Fig. 6) obtenus montrent que le LLM a transformé le funnel webinar en une maquette web concrète en HTML et CSS, fidèle à la structure du parcours défini (Fig.3). La page générée reprend les éléments clés du webinaire (Fig. 3). Au centre de la page, la section principale présente l'étape d'inscription au webinaire. Un indicateur d'étape apparaît en amont du contenu, ce qui permet de situer l'utilisateur dans le processus. Le titre principal annonce clairement l'objectif du webinaire. Un texte descriptif vient ensuite contextualiser le contenu en précisant qu'il s'adresse aux dirigeants et responsables financiers.

Webinar Funnel – Maquettes HTML

Accueil
Inscription
Confirmation
Vidéo 1
Vidéo 2
Vidéo 3
Replay
Automatisation

Étape 1

Inscription au webinar

Comment augmenter votre marge nette de 20 % en 6 mois

Webinaire gratuit pour les dirigeants et responsables financiers qui souhaitent améliorer la rentabilité de leur entreprise sans recruter de nouvelle équipe.

Je réserve ma place

Adresse email

S'inscrire au webinar

Figure 6 : Output numérique (Webinar funnel) généré automatiquement par le LLM

Afin de renforcer la rigueur de la démonstration et d’éviter une lecture uniquement illustrative des résultats, une logique de confrontation analytique a été mobilisée entre les éléments métier attendus dans le webinar funnel initial et les outputs effectivement générés par le LLM. Cette démarche permet d’examiner de manière plus systématique la cohérence des transformations produites au niveau des pages générées, des transitions entre les étapes, des mécanismes d’inscription ainsi que des éléments d’engagement associés au webinar funnel. Le tableau Tab. 4 suivant synthétise cette logique de confrontation analytique en mettant en relation les principaux éléments métier attendus dans le webinar funnel avec les outputs observés dans les artefacts numériques générés par le LLM ainsi que les validations analytiques associées.

Tableau 4 : Validation analytique des transformations du webinar funnel générées par le LLM

Élément métier attendu dans le webinar funnel	Observation dans les outputs générés par le LLM	Validation analytique
Présence d’une page de présentation du webinar	Le LLM génère une landing page HTML/CSS contenant le titre du webinar, une description de l’événement et les informations principales destinées au participant.	La structure métier initiale du webinar funnel est correctement préservée.
Présence d’un formulaire d’inscription	Un formulaire de capture d’email et d’informations	Le mécanisme principal d’inscription au webinar est

	utilisateur apparaît dans la page générée.	conservé dans l'output généré.
Présence d'un bouton d'appel à l'action	Le bouton « S'inscrire maintenant » est intégré dans la structure HTML/CSS générée par le LLM.	Le mécanisme d'engagement et de conversion du webinar funnel reste cohérent avec la logique métier initiale.
Transition vers une page de confirmation	Après validation du formulaire, une redirection vers une page de confirmation est générée.	La continuité logique entre les étapes du funnel est correctement maintenue.
Présence d'un mécanisme de rappel webinar	La page de confirmation contient un mécanisme d'ajout au calendrier et des informations de rappel du webinar.	Les mécanismes de suivi et d'engagement post-inscription sont préservés.
Structuration cohérente des sections HTML/CSS	Les outputs générés contiennent des sections organisées : présentation, formulaire, Call-To-Action, confirmation et informations complémentaires.	Les artefacts numériques générés présentent une structure exploitable et cohérente dans une logique SI orientée digital marketing.
Cohérence globale du parcours utilisateur	Le passage entre les différentes étapes du webinar funnel reste fluide et compréhensible dans les pages générées.	La logique métier globale du webinar funnel demeure cohérente après transformation par le LLM.

Bien que le webinar funnel ait été retenu comme principal cas de démonstration, la logique de transformation étudiée ne se limite pas à cette seule configuration. Dans le cas du webinar funnel, les résultats obtenus montrent qu'un LLM peut structurer plusieurs éléments directement liés au parcours métier initial, notamment une page de présentation du webinar, un formulaire d'inscription, un bouton d'appel à l'action, une page de confirmation ainsi qu'un mécanisme d'ajout au calendrier. Les transitions entre les différentes étapes du funnel restent également cohérentes, en particulier entre l'inscription, la validation du formulaire et la redirection vers la page de confirmation. Une logique similaire peut être mobilisée sur d'autres configurations couramment utilisées dans le marketing digital. Dans le lead funnel, un LLM peut structurer des pages de capture de prospects intégrant des formulaires email, des boutons d'appel à l'action et des mécanismes de redirection entre les différentes étapes du parcours utilisateur. Dans le funnel de vente, il peut également organiser des pages de présentation produit, des boutons de conversion, des formulaires de paiement et des pages de validation de commande tout en maintenant la cohérence des transitions commerciales. Ces résultats

montrent que la logique de transformation étudiée peut être étendue à plusieurs configurations de funnels reposant sur des structures métier et des mécanismes d'interaction différents.

Afin de renforcer la robustesse empirique de la démarche proposée, la logique de transformation étudiée pourrait également être appliquée à d'autres configurations de webinar funnels intégrant des mécanismes complémentaires, tels que des pages de replay, des rappels calendaires ou des étapes de confirmation multi-niveaux. Dans ce type de configuration, un LLM pourrait conserver la cohérence des transitions entre les différentes étapes du funnel, des formulaires d'inscription, des mécanismes d'engagement ainsi que des workflows associés au webinar. Cette possibilité suggère que la logique transformationnelle étudiée ne se limite pas à une seule structure de webinar funnel, mais pourrait être étendue à plusieurs variantes reposant sur des scénarios métier différents.

4.2 Discussion

Les résultats obtenus montrent qu'un LLM peut être utilisé comme un moteur de transformation capable de convertir des funnels marketing en maquettes web structurées en HTML et CSS. Dans ce cadre, le modèle ne fonctionne pas comme un générateur libre, mais comme un mécanisme guidé par une description explicite du funnel et par des règles simples (Vibe coding) qui orientent la production des pages. L'approche proposée repose sur une logique de transformation progressive plutôt que sur des cadres techniques lourds. Cette position intermédiaire permet de conserver une certaine rigueur dans la production tout en bénéficiant de la flexibilité propre aux modèles LLM, ce qui rejoint les travaux récents sur l'utilisation des LLM comme instruments de génération structurée plutôt que comme simples outils de rédaction (Bommasani et al., 2021 ; Wei et al., 2022). Ces résultats suggèrent que le LLM peut servir de médiateur entre une logique marketing et une implémentation web simple. Dès lors que la structure du funnel est explicitement définie, le modèle semble capable de généraliser la transformation à différents scénarios. Cette perspective s'inscrit dans une évolution plus large des usages des LLM vers la génération d'artefacts structurés et orientés processus, déjà observée dans plusieurs travaux récents (Bommasani et al., 2021 ; Zhou et al., 2023).

Les résultats obtenus montrent également que la qualité des artefacts générés dépend fortement du niveau de structuration de la représentation métier initiale ainsi que de la précision des instructions transmises au LLM dans une logique de vibe coding. Une définition incomplète des étapes du funnel ou des transitions associées peut produire des incohérences au niveau des workflows générés, des mécanismes d'inscription ou des interactions entre les différentes pages

produites. Dans cette perspective, le LLM ne remplace pas la logique métier initiale, mais reste fortement dépendant de sa formalisation préalable.

Au-delà des aspects techniques, ces transformations soulèvent également des enjeux organisationnels importants. L'intégration d'artefacts générés par des LLM dans des systèmes d'information orientés digital marketing implique des mécanismes de supervision, de validation et de contrôle des contenus produits. Elle suppose également une adaptation progressive des pratiques de travail, notamment dans les activités liées à la conception des funnels, à la gestion des interactions numériques et à la validation des workflows générés automatiquement.

Ces résultats permettent également de situer cette recherche dans les travaux récents consacrés aux usages des LLM dans les environnements numériques et les systèmes d'information. Alors que plusieurs recherches analysent principalement les capacités des LLM en matière de génération de contenu ou d'assistance conversationnelle, les résultats obtenus ici mettent davantage l'accent sur leur capacité à intervenir dans un processus de transformation structuré reliant une représentation métier orientée webinar funnel à des artefacts numériques exploitables. Les expérimentations réalisées montrent notamment que le LLM peut préserver des éléments directement liés à la logique métier du funnel, tels que les transitions entre les étapes, les mécanismes d'inscription, les formulaires de capture ou les interactions associées aux workflows du webinar. Dans cette perspective, le rôle du LLM dépasse une simple fonction de génération textuelle et s'inscrit davantage dans une logique de médiation entre structuration métier et implémentation numérique orientée système d'information.

4.3 Limitations

Plusieurs limites doivent être prises en compte dans l'utilisation d'un LLM pour transformer des funnels marketing en pages web HTML et CSS. Une première limite concerne la qualité de la description du funnel. Le LLM peut produire des interfaces qui ne reflètent pas correctement la logique du parcours. Une autre limite est liée à la nature probabiliste du modèle. Une limite supplémentaire réside dans le phénomène d'hallucination. Il convient également de souligner les risques liés à la sécurité et à la confidentialité des informations. La gestion des données doit donc rester prudente et maîtrisée. Enfin, le périmètre de l'expérimentation reste restreint, puisqu'il s'appuie principalement sur le Webinar Funnel.

4. 4 Risques des LLM et management de changement

Sur le plan de la sécurité de l'information, les principes portés par la norme ISO 27001 restent essentiels. Les données utilisées dans les funnels peuvent contenir des informations sensibles,

ce qui implique un contrôle strict des accès, une traçabilité des interactions et une gestion claire des responsabilités. Des référentiels comme l'ISO 23001 rappellent aussi l'importance d'anticiper les risques opérationnels et de maintenir une continuité dans les processus numériques qui reposent sur l'IA.

Au-delà des aspects techniques, l'introduction des LLM transforme les pratiques de travail et demande un effort clair de management de changement. Plusieurs résistances apparaissent souvent. Ces réactions sont normales et doivent être intégrées dans la stratégie d'adoption. Pour accompagner cette évolution, quelques leviers simples mais structurants peuvent être mobilisés. Une communication transparente sur les objectifs et les bénéfices attendus permet de réduire les inquiétudes. Une formation progressive aide les équipes à s'appropriier les usages sans pression excessive. L'implication des parties prenantes dès le début du projet renforce l'adhésion et favorise une meilleure compréhension des transformations en cours.

4. Conclusion

Dans cet article, nous avons analysé l'évolution de l'automatisation du marketing digital à la lumière des apports récents des LLM. Nous avons structuré notre réflexion à partir d'une revue de la littérature portant à la fois sur le marketing automation, sur le rôle croissant des LLM dans les systèmes d'information et sur les enjeux de sécurité et de management de changement. Nous avons défini l'automatisation du marketing digital comme une capacité organisationnelle fondée sur l'orchestration du funnel et l'exécution automatisée des interactions. Nous avons montré que le funnel marketing constitue aujourd'hui l'architecture managériale centrale de cette automatisation, tandis que l'IA agit comme moteur transversal d'optimisation. Dans une perspective de DSR, nous avons conçu des artefacts orientés métier afin de formaliser le funnel marketing digital. Nous avons adopté une posture constructiviste dans laquelle la conception d'artefacts sert à comprendre et structurer une problématique organisationnelle. Nous avons distingué trois configurations représentatives : le funnel de vente, le lead funnel et le webinar funnel. Nous avons ensuite mobilisé un modèle de langage comme mécanisme de transformation des artefacts conçus. Nous avons démontré que, lorsqu'il est guidé par une description explicite du funnel et par des règles simples, le LLM peut convertir une représentation marketing structurée en une maquette web opérationnelle en HTML et CSS.

À travers cette recherche, nous avons ainsi contribué à clarifier le rôle des LLM comme médiateurs entre logique marketing et implémentation numérique, tout en mettant en évidence les conditions organisationnelles nécessaires pour une automatisation responsable et cohérente.

Cette recherche présente plusieurs apports complémentaires. Sur le plan théorique, elle contribue à préciser le rôle des LLM comme mécanismes de médiation entre représentations métier orientées funnels marketing et artefacts numériques exploitables dans des systèmes d'information orientés digital marketing. Sur le plan méthodologique, elle montre l'intérêt d'une approche fondée sur le Design Science Research pour formaliser et transformer des artefacts métier dans une logique de génération assistée par LLM. Sur le plan managérial, les résultats mettent en évidence les enjeux liés à la gouvernance des données, à la supervision des artefacts générés et au management du changement dans les processus d'automatisation du marketing digital.

Plusieurs perspectives peuvent prolonger cette recherche. Une première piste concernerait l'intégration de mécanismes de Retrieval-Augmented Generation (RAG) afin d'améliorer la cohérence des transformations produites à partir de bases de connaissances métier structurées. Une autre perspective porterait sur l'utilisation d'architectures agentiques capables d'orchestrer automatiquement différentes étapes de transformation des funnels marketing, notamment dans des workflows multi-étapes orientés systèmes d'information. Des travaux futurs pourraient également approfondir l'évaluation de ces transformations dans des environnements organisationnels réels afin d'analyser plus finement les enjeux liés à la gouvernance, à la supervision des artefacts générés et à l'appropriation organisationnelle des systèmes fondés sur les LLM.

5. Bibliographie

- Baskerville, R., Kaul, M., & Storey, V. (2018). Genres of inquiry in design-science research. *MIS Quarterly*, 42(3), 1–18.
- Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). On the dangers of stochastic parrots: Can language models be too big? In *Proceedings of the 2021 ACM (FAccT '21)* (pp. 610–623). <https://doi.org/10.1145/3442188.3445922>
- Bleier, A., Harmeling, C. M., & Palmatier, R. W. (2019). Creating effective online customer experiences. *Journal of Marketing*, 83(2), 98–119. <https://doi.org/10.1177/0022242918809930>
- Bommasani, R., Hudson, D. A., Adeli, E., Altman, R., Arora, S., von Arx, S., Bernstein, M. S., Bosselut, A., Brunskill, E., Brynjolfsson, E., et al. (2021). On the opportunities and risks of foundation models. *arXiv*. <https://doi.org/10.48550/arXiv.2108.07258>

- Cillo, P., & Rubera, G. (2024). Generative AI in innovation and marketing processes: A roadmap of research opportunities. <https://doi.org/10.1007/s11747-024-01044-7>
- Colicev, A., Kumar, A., & O'Connor, P. (2019). Modeling the relationship between firm and user generated content and the stages of the marketing funnel. *International Journal of Research in Marketing*, 36(1), 100–116. <https://doi.org/10.1016/j.ijresmar.2018.09.005>
- Court, D., Elzinga, D., Mulder, S., & Vetvik, O. (2009). The consumer decision journey. *McKinsey Quarterly*.
- Dwivedi, Y. K., Kshetri, N., Hughes, L., et al. (2023). So what if ChatGPT wrote it? *International Journal of Information Management*, 71, 102642. <https://doi.org/10.1016/j.ijinfomgt.2023.102642>
- Estevez, M., Ballestar, M. T., & Sainz, J. (2025). Market research and knowledge using generative AI: The power of large language models. *Journal of Innovation & Knowledge*. <https://doi.org/10.1016/j.jik.2025.100796>
- Feuerriegel, S., Hartmann, J., Janiesch, C., & Zschech, P. (2024). Generative AI. *Business & Information Systems Engineering*. <https://doi.org/10.1007/s12599-023-00834-7>
- Ferrag, M. A., Alwahedi, F., Battah, A., Cherif, B., Mechri, A., Tihanyi, N., Bisztray, T., & Debbah, M. (2025). Generative AI in cybersecurity: A comprehensive review of LLM applications and vulnerabilities. <https://doi.org/10.1016/j.iotcps.2025.01.001>
- Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS Quarterly*, 37(2), 337–355.
- Grewal, D., Saturnino, C. B., Davenport, T. H., & Guha, A. (2025). How generative AI is shaping the future of marketing. *Journal of the Academy of Marketing Science*, 53(3), 702–722. <https://doi.org/10.1007/s11747-024-01064-3>
- Guercini, S. (2023). Marketing automation and the scope of marketers' heuristics. *Management Decision*, 61(13), 295–320. <https://doi.org/10.1108/MD-07-2022-0909>
- Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, 28(1), 75–105.
- Iivari, J. (2015). Distinguishing and contrasting two strategies for design science research. *European Journal of Information Systems*, 24(1), 107–115.

- Kanbach, D. K., Heiduk, L., Blueher, G., Schreiter, M., & Lahmann, A. (2024). The GenAI is out of the bottle: Generative artificial intelligence from a business model innovation perspective. *Review of Managerial Science*. <https://doi.org/10.1007/s11846-023-00696-z>
- Kotler, P., & Keller, K. L. (2016). *Marketing management* (15th ed.). Pearson.
- Kotter, J. P. (1995). Leading change: Why transformation efforts fail. *Harvard Business Review*, March–April, 59–67.
- Kumar, V., Ashraf, A. R., & Nadeem, W. (2024). AI-powered marketing: What, where, and how? *International Journal of Information Management*, 77, 102783. <https://doi.org/10.1016/j.ijinfomgt.2024.102783>
- Madhushan, M. I., Abeywickrama, H. N., & Sumanasiri, E. A. G. (2024). An examination of digital marketing as a tool to enhance customer engagement in the hotel industry: A case study of the Western Province, Sri Lanka. *Asian Journal of Marketing Management (AJMM)*, 3(2), 97–123.
- March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems*, 15(4), 251–266.
- Mero, J., Leinonen, M., Makkonen, H., & Karjaluoto, H. (2022). Agile logic for SaaS implementation: Capitalizing on marketing automation software in a start-up. *Journal of Business Research*, 145, 583–594. <https://doi.org/10.1016/j.jbusres.2022.03.026>
- Palos-Sanchez, P., Saura, J. R., & Martin-Velicia, F. (2019). A study of the effects of programmatic advertising on users' concerns about privacy overtime. *Journal of Business Research*, 96, 61–72. <https://doi.org/10.1016/j.jbusres.2018.10.059>
- Peggiani, G., & Lamberti, L. (2026). Beyond the post: Crafting influencer marketing strategies across the funnel. *Journal of Business Research*, 207, Article 116037. <https://doi.org/10.1016/j.jbusres.2026.116037>
- Peppers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, 24(3), 45–77.
- Salonen, A., Järvinen, J., Munnukka, J., Zimmer, M., & Karjaluoto, H. (2024). Digital content marketing on social media along the B2B customer journey: The effect of timely content

- delivery on customer engagement. *Industrial Marketing Management*, 118, 12–26. <https://doi.org/10.1016/j.indmarman.2024.02.002>
- Shankar, V., Grewal, D., Sunder, S., Fossen, B., Peters, K., & Agarwal, A. (2022). Digital marketing communication in global marketplaces: A review of extant research. *International Journal of Research in Marketing*, 39(2), 541–565. <https://doi.org/10.1016/j.ijresmar.2021.09.005>
- Silva, S. C., Corbo, L., Vlačić, B., & Fernandes, M. (2023). Marketing accountability and marketing automation. *EuroMed Journal of Business*. <https://doi.org/10.1108/EMJB-11-2020-0117>
- Simon, H. A. (1996). *The sciences of the artificial* (3rd ed.). MIT Press.
- Taeihagh, A. (2025). Governance of generative AI. *Policy and Society*. <https://doi.org/10.1093/polsoc/puaf001>
- Thomaz, F., Salge, C., Karahanna, E., & Hulland, J. (2020). Learning from the dark web: Leveraging conversational agents in the era of hyper-privacy to enhance marketing. *Journal of the Academy of Marketing Science*, 48(1), 43–63. <https://doi.org/10.1007/s11747-019-00704-3>
- van Aken, J. E. (2004). Management research based on the paradigm of the design sciences. *Journal of Management Studies*, 41(2), 219–246.
- Verhoef, P. C., Broekhuizen, T., Bart, Y., et al. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*, 122, 889–901. <https://doi.org/10.1016/j.jbusres.2019.09.022>
- Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *MIS Quarterly*, 43(1), 118–144. <https://doi.org/10.25300/MISQ/2019/13375>
- Weidig, J., Weippert, M., & Kuehnl, C. (2024). Personalized touchpoints and customer experience: A conceptual synthesis. *Journal of Business Research*, 177, Article 114641. <https://doi.org/10.1016/j.jbusres.2024.114641>
- Weidinger, L., Mellor, J., Rauh, M., et al. (2022). Ethical and social risks of harm from language models. *arXiv preprint arXiv:2112.04359*. <https://arxiv.org/abs/2112.04359>

Wei, J., Wang, X., Schuurmans, D., Bosma, M., Ichter, B., Xia, F., Chi, E., Le, Q. V., & Zhou, D. (2022). Chain-of-thought prompting elicits reasoning in large language models. arXiv. <https://doi.org/10.48550/arXiv.2201.11903>

Zhou, D., Schärli, N., Hou, L., Wei, J., Scales, N., Wang, X., Schuurmans, D., Cui, C., Bousquet, O., Le, Q. V., & Chi, E. (2022). DOI: <https://doi.org/10.48550/arXiv.2205.10625>

CHAPITRE 10 : *Gestion du risque opérationnel lié au facteur humain dans les banques marocaines : analyse qualitative du rôle des pratiques RH*

TAMI Amina

Doctorante, Laboratoire Universitaire de Recherche en Instrumentation et Gestion des Organisations-FSJESO- amina.tami.1.24@ump.ac.ma

SAKHRAOUI Bahija

Enseignante Chercheure, Laboratoire Universitaire de Recherche en Instrumentation et Gestion des Organisations -FSJESO- bsakhraoui1@gmail.com

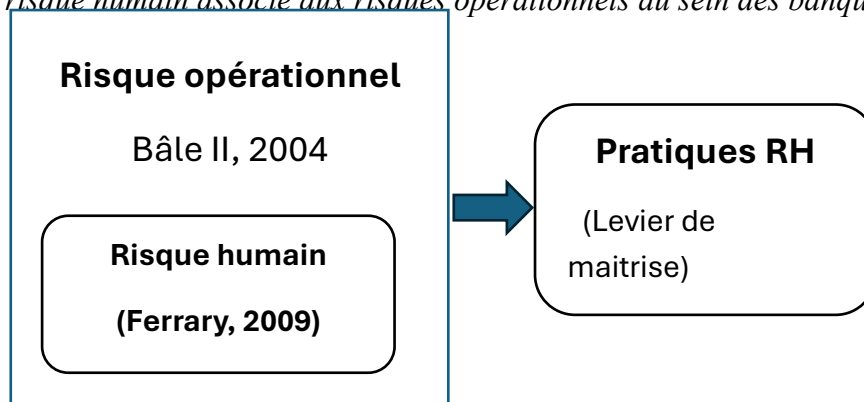
Les pertes opérationnelles liées au facteur humain représentent l'une des principales sources de vulnérabilité dans le secteur bancaire mondial. Erreurs de procédure, fraudes internes, départs de collaborateurs stratégiques, conflits sociaux : autant de situations qui peuvent fragiliser durablement un établissement, indépendamment de la solidité de son bilan. Dans un secteur où la masse salariale constitue le premier poste de coût et où la création de valeur repose largement sur le capital humain, ignorer cette dimension serait une erreur de gouvernance.

Le risque opérationnel, tel que défini par le Comité de Bâle (2004), couvre précisément les pertes résultant de défaillances internes humaines, organisationnelles ou techniques, ainsi que d'événements extérieurs. Cette définition place le facteur humain au cœur du dispositif de gestion des risques, non comme une variable périphérique, mais comme une composante structurelle. Les scandales financiers et les dysfonctionnements observés dans les établissements bancaires ont d'ailleurs confirmé les limites des approches purement techniques ou réglementaires : sans une gestion efficace du capital humain, aucun dispositif de contrôle ne suffit.

Au Maroc, la question prend une dimension particulière. Bank Al-Maghrib a progressivement renforcé le cadre prudentiel en transposant les exigences de Bâle II et Bâle III, avec des ratios de solvabilité parfois plus contraignants que les standards internationaux. Pourtant, la littérature académique sur le risque humain dans les banques marocaines reste peu développée, et l'articulation entre pratiques RH et gestion des risques opérationnels y est encore peu explorée empiriquement.

C'est précisément ce manque que cet article cherche à combler. En s'appuyant sur les travaux fondateurs de Ferrary (2009) sur les ressources humaines à risque, enrichis par la théorie des ressources et compétences (Barney, 1991) et les apports de la résilience organisationnelle, il propose une lecture intégrée du risque humain de ses typologies à ses mécanismes de prévention. La question centrale est la suivante :

Dans quelle mesure les politiques et pratiques de ressources humaines peuvent-elles contribuer à gérer le risque humain associé aux risques opérationnels au sein des banques marocaines ?



Trois hypothèses de recherche structurent cette réflexion :

- H1 : La formation continue et la gestion des compétences réduisent le risque d'erreur humaine et renforcent la culture du risque au sein des banques marocaines.
- H2 : Les politiques de rémunération incitatives et les dispositifs de fidélisation limitent les risques de malversation et de perte de ressources stratégiques.

- H3 : La coordination entre la fonction RH, la direction des risques et l'audit interne contribue à l'émergence d'une culture organisationnelle du risque partagée.

Pour répondre à ces hypothèses, une démarche qualitative exploratoire a été adoptée, fondée sur dix entretiens semi-directifs conduits auprès de professionnels bancaires marocains aux profils variés directeurs généraux, responsables RH, gestionnaires des risques, managers opérationnels et contrôleurs internes. Les données ont été analysées par une méthode d'analyse thématique de contenu, en cohérence avec la nature exploratoire de la recherche.

L'article s'organise en deux temps : une revue de littérature structurée autour des concepts de risque opérationnel, de risque humain et de pratiques RH, suivie d'une analyse empirique des résultats issus du terrain bancaire marocain.

Cadre théorique

Cet article se situe à l'intersection de deux champs disciplinaires : le management des risques opérationnels et la gestion stratégique des ressources humaines. Il s'appuie sur les travaux de Ferrary (2009) sur les typologies du risque humain, enrichis par la théorie des ressources et compétences (Barney, 1991) et la résilience organisationnelle (Weick & Sutcliffe, 2001), pour construire un cadre analytique qui articule pratiques RH et prévention du risque opérationnel.

1. Ancrages théoriques mobilisés

Trois corpus théoriques structurent ce travail. Chacun répond à une question précise que pose le sujet.

1.1 La théorie des ressources et compétences (Resource-Based View)

Développée par Penrose (1959) et formalisée par Barney (1991) dans *"Firm Resources and Sustained Competitive Advantage"*, la Resource-Based View postule que l'avantage concurrentiel durable d'une organisation repose sur des ressources internes rares, difficilement imitables et non substituables résumées sous l'acronyme VRIN.

Appliquée au capital humain, cette théorie change le regard qu'on porte sur certains collaborateurs : ils ne sont pas simplement des coûts à optimiser, ce sont des actifs stratégiques dont la perte expose directement l'organisation à un risque compétitif. Dans le secteur bancaire, elle fonde la distinction entre ressources humaines ordinaires et ressources humaines stratégiques, et justifie l'investissement dans des dispositifs spécifiques de rétention, de développement et de planification de la succession.

1.2 La théorie des incitations et la relation d'agence

Issue des travaux fondateurs de Jensen & Meckling (1976) dans *"Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure"*, la théorie de l'agence analyse les conditions dans lesquelles les intérêts des salariés peuvent diverger de ceux de

l'organisation. Cette divergence appelée problème d'agence est au cœur du risque de malversation bancaire.

La théorie postule qu'un collaborateur adopte des comportements conformes aux objectifs de son employeur lorsque son contrat augmente les coûts des comportements déviants et réduit les gains potentiels de la fraude.

Des travaux empiriques récents Abdullahi & Mansor (2015) et Khanna & Arora (2009) confirment que les dispositifs organisationnels fondés sur cette logique sont plus efficaces que les sanctions seules pour réduire durablement le risque de fraude interne.

1.3 La résilience organisationnelle

Conceptualisée par Weick & Sutcliffe (2001) dans *"Managing the Unexpected: Assuring High Performance in an Age of Complexity"*, la résilience organisationnelle désigne la capacité d'une organisation à anticiper les perturbations, absorber les chocs et se reconfigurer face à l'adversité. Elle s'inscrit dans le cadre des organisations hautement fiables (High Reliability Organizations), qui opèrent dans des environnements complexes et à fort risque dont le secteur bancaire est un exemple emblématique.

Appliquée à notre sujet, cette théorie déplace le regard : la maîtrise du risque humain ne repose pas uniquement sur des mécanismes de contrôle réactifs. Elle suppose une culture organisationnelle proactive capable à détecter les signaux faibles, distribuer les compétences critiques, éviter les dépendances individuelles et maintenir une capacité d'adaptation face aux perturbations (Hollnagel et al., 2006).

1.4 Articulation des trois ancrages

Ces trois théories ne se substituent pas elles se complètent. La RBV explique *pourquoi* certains profils humains sont stratégiques. La théorie des incitations explique *comment* aligner les comportements individuels sur les objectifs organisationnels. La résilience organisationnelle explique *dans quel environnement culturel* ces mécanismes deviennent efficaces et durables. Ensemble, ils offrent un cadre intégré pour analyser le lien entre pratiques RH et gestion du risque opérationnel.

2. Le management des risques

La gestion des risques s'est imposée comme outil stratégique de pilotage à la suite des grandes crises financières et des faillites d'entreprise. Initialement centrée sur les assurances aux États-Unis dans les années 1950-60, elle s'est progressivement élargie pour couvrir l'ensemble des risques organisationnels financiers, opérationnels, stratégiques, réputationnels. Elle ne vise pas à éliminer le risque, mais à permettre une prise de risque consciente et maîtrisée.

Ce qui caractérise une gestion des risques mature, c'est son refus du découpage en silos. Les approches fragmentées dispersent les responsabilités, réduisent la visibilité globale et

augmentent mécaniquement l'exposition aux risques inutiles. Plusieurs cadres institutionnels illustrent cette logique intégrée, résumés dans le Tableau 1.

Tableau 1 : Les définitions du Risk Management

Auteur	Définition
Committee of Sponsoring Organizations of the Treadway Commission (COSO)	Processus conçu pour identifier, gérer et surveiller les risques afin d'assurer la réalisation des objectifs de l'organisation.
Institute of Risk Management (IRM)	Processus qui vise à aider les organisations à comprendre, évaluer et agir sur l'ensemble de leurs risques en vue d'augmenter la probabilité de succès et de réduire la probabilité d'échec
Institute of Internal Auditors (IIA)	Approche rigoureuse et coordonnée pour évaluer et répondre à tous les risques affectant l'atteinte des objectifs stratégiques et financiers
HM Treasury	Ensemble de processus incluant l'identification, l'évaluation, l'attribution des responsabilités, la prise de mesures correctives et le suivi des progrès.

Source : Elaboré par nos soins sur la base des travaux de HM Treasury.

Ainsi conçue, la gestion des risques constitue un outil d'aide à la décision stratégique permettant d'améliorer la qualité des décisions, de réduire l'incertitude, de sécuriser les processus clés et d'optimiser l'allocation des ressources. Dans ce cadre global, le risque opérationnel représente une catégorie majeure, directement liée à la continuité des activités et illustrant concrètement l'application des principes du Risk Management.

2.1. Le risque opérationnel bancaire

Le risque opérationnel désigne le risque de pertes résultant de défaillances dans les processus internes, les systèmes, les personnes, ou d'événements externes (Timsit, 2010). Dans le secteur bancaire, Bâle II le définit comme *"le risque de pertes résultant de processus internes inadéquats ou défaillants, de personnes et de systèmes, ou d'événements externes"*. Bien que moins fréquent que les risques de crédit ou de marché, sa survenance peut être dévastatrice et il ne peut être ni plafonné ni transféré via les marchés financiers (Thirlwell, 2010).

Les chiffres le confirment : selon le Basel Committee on Banking Supervision (2021), le facteur humain est impliqué dans près de 60% des incidents opérationnels déclarés par les établissements bancaires mondiaux. Des travaux empiriques récents, notamment Chernobai et al. (2011), montrent que les défaillances humaines constituent la principale source de pertes opérationnelles dans les banques de détail. Dans le contexte marocain, Bank Al-Maghrib (2024) souligne que les dispositifs de contrôle interne restent

insuffisamment articulés avec la gestion des ressources humaines une zone de vulnérabilité structurelle qui motive directement cette recherche.

2.2. Le risque humain et ses typologies

"Les risques humains sont spécifiques dans la mesure où ils sont liés à l'usage d'une ressource douée d'une volonté propre, dotée d'une stratégie personnelle qui peut diverger de celle de son employeur" (Crozier & Friedberg, 1977). Contrairement aux risques techniques ou systémiques, le risque humain ne peut être ni totalement éliminé par la procédure, ni réduit à une probabilité statistique. Il s'inscrit dans la relation de travail elle-même.

Ferrary (2009) identifie cinq typologies du risque humain qui structurent l'analyse qui suit, enrichies par des travaux empiriques récents.

2.2.1. Le risque de perte de ressources humaines stratégiques

L'avantage concurrentiel d'une banque repose largement sur des ressources humaines rares, difficilement imitables et non substituables ce que Barney (1991) qualifie de ressources stratégiques au sens de la RBV. Perdre un collaborateur détenteur de savoirs tacites critiques, c'est perdre plus qu'un poste : c'est perdre une partie de l'avantage concurrentiel.

Dans le secteur bancaire, le taux de départ des cadres constitue un indicateur avancé de ce risque. Des travaux récents Alias et al. (2016) confirment que la rétention des talents reste un défi structurel, particulièrement dans les fonctions à forte technicité. La réponse passe par des politiques de rémunération incitatives, salaire variable, actionnariat salarié, stock-options conçues pour aligner les intérêts des collaborateurs avec ceux de l'organisation.

2.2.2. Le risque de disparition de ressources humaines spécifiques

Au-delà du départ volontaire, les organisations peuvent perdre des collaborateurs détenteurs de compétences rares, non transférables à court terme (Becker, 1962). Ce risque est aggravé par deux dynamiques convergentes : les vagues de retraites dans les fonctions expertes et la digitalisation, qui crée des besoins en compétences hybrides difficiles à pourvoir rapidement.

Les mécanismes de prévention opèrent à trois niveaux : identification préventive des compétences critiques via la cartographie des emplois, plans de succession et assurance homme-clé, et GPEC comme dispositif structurel d'anticipation et de transmission des savoirs.

2.2.3. Le risque d'erreur humaine

Le risque d'erreur est la catégorie la plus fréquente du risque humain en banque. Erreurs de saisie, non-respects de procédures, défaillances dans la gestion des dossiers de crédit. Ses manifestations sont multiples, ses conséquences variables : de l'incident mineur au litige juridique en passant par l'atteinte réputationnelle.

Ce risque est généralement involontaire. Le modèle du "fromage suisse" de Reason (1990) l'illustre bien : les erreurs humaines résultent d'une combinaison de défaillances systémiques et individuelles, rarement d'un fait isolé. Cette perspective est particulièrement pertinente dans les banques, où les processus sont fortement

interdépendants. Les leviers de prévention sont la standardisation, la formation continue, la dématérialisation et le double contrôle doivent donc être pensés en système, pas en actions ponctuelles.

2.2.4. Le risque de malversation

Le Comité de Bâle (2003) intègre explicitement la fraude interne dans le périmètre du risque opérationnel. Le risque de malversation découle de comportements volontairement frauduleux : manipulations comptables, détournements, délits d'initié, pouvant générer des pertes majeures et des crises de réputation durables.

La théorie des incitations (Jensen & Meckling, 1976) offre le cadre analytique le plus pertinent : un collaborateur est moins susceptible de frauder si son contrat augmente les coûts de la malversation tout en réduisant les gains potentiels. Abdullahi & Mansor (2015) et Khanna & Arora (2009) le confirment empiriquement : les dispositifs organisationnels contrôle interne, culture éthique, politique RH cohérente sont plus efficaces que les sanctions seules. L'actionnariat salarié, la séparation des fonctions, la rotation des postes sensibles et l'automatisation des processus constituent les principaux leviers identifiés.

2.2.5. Le risque de conflit

Le risque de conflit découle du pouvoir de négociation des collaborateurs, individuel ou collectif. Les salariés détenteurs de compétences stratégiques peuvent exercer une pression significative allant jusqu'au blocage d'activités critiques ou à des atteintes réputationnelles.

Ce risque s'inscrit directement dans le prolongement de Crozier & Friedberg (1977) : plus un collaborateur contrôle une ressource rare et non substituable, plus son pouvoir de négociation est élevé. La résilience organisationnelle (Weick & Sutcliffe, 2001) apporte ici une perspective complémentaire : les organisations résilientes parviennent à distribuer les compétences critiques, éviter les dépendances individuelles et maintenir une capacité d'adaptation face aux perturbations. Les leviers de prévention combinent cartographie des compétences, suivi des indicateurs de climat social, politiques de rémunération équitables et digitalisation des processus.

Les cinq typologies de Ferrary (2009) ne sont pas indépendantes elles s'alimentent mutuellement. Un risque stratégique non maîtrisé peut générer un risque de conflit ; un risque d'erreur récurrent peut révéler un risque de disparition de compétences. C'est cette interdépendance qui justifie une approche intégrée, articulant pratiques RH et dispositifs de gestion des risques opérationnels.

Le modèle conceptuel proposé formalise ces relations : les pratiques RH agissent sur chaque type de risque humain, qui alimente à son tour le risque opérationnel. La culture organisationnelle du risque construite par la coordination entre la fonction RH, la direction des risques et l'audit interne constitue le mécanisme intérateur central de ce modèle.

3. Méthodologie de recherche

Les méthodes qualitatives permettent d'analyser en profondeur les phénomènes organisationnels dans leur contexte et de comprendre les perceptions et attitudes des acteurs. Dans cette perspective, notre recherche empirique est basée sur une démarche qualitative exploratoire s'appuyant sur des entretiens semi-directifs menés auprès de professionnels du secteur bancaire, afin d'identifier, par une analyse thématique de contenu, les pratiques de ressources humaines susceptibles d'influencer la gestion du risque humaine lié au risque opérationnel bancaire.

Cette étude adopte une démarche exploratoire, justifiant une certaine flexibilité dans la conduite des entretiens afin de favoriser des discours spontanés et authentiques. Un guide d'entretien a néanmoins été conçu pour encadrer les échanges et assurer leur cohérence, sans en limiter la dynamique. Les entretiens semi-directifs réalisés ont ainsi permis d'aborder les principales thématiques liées à l'objet de recherche. Le Tableau 2, présente les caractéristiques générales de nos 10 cas étudiées :

Méthodes de recueil	Les entretiens semi-directifs
Durée	40-45 minutes
Profil des répondants	-Directeur Général / Directeur de banque -Directeur des Ressources Humaines -Responsable RH -Responsable de formation /Développement des compétences -Responsable gestion des risques -Manager opérationnel -Responsable agence -Contrôleur permanent et gestionnaire... -Cadre
Nombre de cas étudiées	10 entretiens
Guide de recueil des données	-Thème 1 : Rôle stratégique de la fonction RH -Thème 2 : Profils stratégiques et continuité d'activité -Thème 3 : Fraude interne et mesures de prévention -Thème 4 : Erreurs humaines et conflits

4. Présentation des résultats de l'étude qualitative exploratoire

Dans le secteur bancaire, fortement exposé aux risques opérationnels, la maîtrise du risque humain constitue un enjeu stratégique central. Les pratiques de gestion des ressources humaines, jouent un rôle déterminant dans la prévention et l'encadrement de ces risques. Leur intégration dans la gouvernance des banques contribue au renforcement de la culture du risque et à l'amélioration de la performance organisationnelle, en particulier dans le contexte marocain.

Suite à des entretiens semi-directifs réalisés auprès des acteurs bancaires marocains interviewés, nous avons pu relever, les résultats de recherche suivants :

4.1. Rôle stratégique de la fonction RH

En premier lieu, les résultats mettent en évidence le rôle déterminant de la fonction ressources humaines dans la maîtrise du risque humain, à travers différentes pratiques mises en œuvre au sein de l'organisation, comme l'illustrent les verbatims suivants :

« La fonction RH au sein de notre établissement contribue à la prévention du risque humain à travers un recrutement rigoureux ainsi qu'une gestion des compétences professionnelles par la mise en place des plans de formation continue et elle mène des actions de sensibilisation en faveur des collaborateurs pour qu'ils adoptent un comportement responsable toute en collaborant avec la direction risques et la direction audit interne »

« La fonction ressources humaines joue un rôle stratégique et essentiel dans la prévention des risques et ceci notamment à travers le respect du statut du personnel, tout en garantissant une gestion efficace des carrières et des aspects sociaux des ressources humaines »

« ... Sensibilisation des managers au management responsable, promotion de valeurs partagées telles que le respect, l'inclusion et la transparence, et coordination avec les autres directions (sécurité, juridique, communication) ».

4.2. Profils stratégiques et continuité d'activité

Dans un second temps, les échanges avec les répondants montrent que, bien que l'ensemble des postes bancaires soit exposé aux risques, certains profils occupent une position particulièrement sensible. Ces postes, en raison de leurs responsabilités et de leur degré d'exposition, concentrent davantage de risques humains, comme en témoignent les verbatims présentés ci-après :

« Sont considérés comme profils stratégiques au sein de notre organisation les Directeurs d'agences et les chargés de clientèle puisqu'ils détiennent un portefeuille de clients importants qui pourrait impacter négativement l'activité et la performance de notre entreprise ».

« Dans une banque, plusieurs profils sont considérés comme stratégiques car ils contribuent directement à la performance commerciale, à la maîtrise des risques ou à la transformation digitale Exemple : Traders, analystes risque, chargés d'affaire, experts conformité ... ».

« Le médecin du travail joue un rôle essentiel dans la prévention du risque humain. Son intervention permet de détecter précocement des anomalies sanitaires chez les employés, ce qui contribue à limiter les situations à risque au sein de la banque ».

✓ Mesures pour sécuriser les profils stratégiques

Les résultats recueillis auprès des répondants mettent en évidence les pratiques mises en œuvre par les banques pour sécuriser et fidéliser leurs collaborateurs stratégiques. Celles-ci portent à la fois sur la rémunération et la reconnaissance, mais aussi sur la gestion des postes clés, à travers la formation, les plans de relève, la documentation des procédures et la mise en place d'intérim.

« La rétention des salariés stratégiques repose sur une combinaison entre salaire fixe et salaire variable, permettant d'ajuster la reconnaissance en fonction de la performance. »

« Les primes, les bonifications et les challenges constituent des leviers importants de reconnaissance et de motivation pour les profils stratégiques. »

« La banque met en place plusieurs dispositifs pour sécuriser ses postes clés : identifier des remplaçants internes à travers des plans de relève, documenter les procédures, prévoir des intérim en cas d'absence soudaine, et développer les compétences des collaborateurs par la formation afin de préparer leur évolution vers des postes stratégiques. »

4.3. Fraude interne et mesures de prévention

Les postes les plus exposés à la fraude bancaire identifiés par les répondants comprennent principalement la gestion des comptes clients et les guichets, l'analyse des dossiers de crédit et financement, ainsi que la trésorerie et les marchés financiers. Pour prévenir ces risques, plusieurs mesures sont mises en œuvre, telles que le renforcement du contrôle interne, la formalisation des procédures, la séparation des tâches, la rotation des postes sensibles, la formation et la sensibilisation, l'instauration de sanctions disciplinaires, l'automatisation des processus, ainsi que des dispositifs de rémunération et de reconnaissance. Ces mesures seront présentées plus en détail à travers les verbatims suivants.

« Pour limiter les risques de fraude, nous appliquons un contrôle interne strict avec des procédures formalisées, et nous veillons à ce que les responsabilités clés soient réparties entre plusieurs collaborateurs afin d'éviter tout abus ».

« Les postes les plus exposés, comme la caisse, le crédit ou la trésorerie, sont régulièrement occupés par différents collaborateurs. Cette rotation permet de réduire les risques et d'assurer une vigilance constante ».

« Nous investissons dans la formation et la sensibilisation des employés, en développant à la fois leurs compétences techniques et leur conscience éthique pour prévenir les comportements à risque ».

« ... En complément, des sanctions disciplinaires sont prévues en cas de manquement, certains processus sont automatisés pour limiter les erreurs humaines, et les collaborateurs sont encouragés et fidélisés grâce à des dispositifs de rémunération combinant salaire fixe, variable et primes. »

4.4. Erreurs humaines et conflits

Les erreurs humaines représentent un risque majeur pour les banques, pouvant affecter la qualité des opérations et la sécurité des transactions. Les acteurs bancaires interviewés ont identifié plusieurs facteurs principaux qui favorisent ces erreurs, liés aux conditions de travail et à la maîtrise des processus.

✓ Sources d'erreurs humaines

« *Le stress et la pression sont vraiment pesants dans notre quotidien. Avec les délais serrés et les objectifs trop élevés, il est facile de faire des erreurs sans s'en rendre compte.* »

« *Les procédures sont trop compliquées et parfois mal expliquées. Même quand on croit bien les connaître, on peut se tromper dans les étapes.* »

« *Beaucoup de collègues n'ont pas reçu la formation nécessaire pour certaines opérations. Sans les compétences adaptées, les erreurs arrivent rapidement.* »

« *Souvent, la supervision est insuffisante. Les contrôles de premier niveau ne détectent pas toutes les erreurs, et elles se propagent dans le processus.* »

« *Il arrive que les systèmes informatiques nous jouent des tours. Une mauvaise saisie ou un bug peut créer des problèmes importants, comme des virements erronés ou des absences d'ordre écrit.* »

« *On voit parfois des erreurs de calcul ou des détournements, surtout quand plusieurs facteurs se combinent : surcharge, complexité des tâches et manque de contrôle.* »

✓ Mesures pour maîtriser le risque d'erreur humaine

Pour limiter ces erreurs, les acteurs bancaires interviewés ont proposé plusieurs mesures, centrées sur la communication, la formation, la clarté des responsabilités et le développement des compétences :

« *... Il faut renforcer le dialogue entre équipes et avec la direction. Quand on parle des problèmes ouvertement, on peut prévenir beaucoup d'erreurs.* »

« *L'équité dans la gestion des promotions, sanctions et évaluations est essentielle. Si les règles sont appliquées de manière transparente, les collaborateurs travaillent plus sereinement et font moins d'erreurs...* ».

« *Notre organisation déploie plusieurs actions structurées pour réduire et maîtriser les erreurs humaines. Elle renforce d'abord la culture du risque à travers des formations régulières et ciblées. Elle met également en place des procédures opérationnelles clarifiées, accompagnées d'outils de contrôle interne et de double vérification.* ».

« *L'automatisation des processus répétitifs aide énormément. Quand les tâches routinières sont automatisées, les erreurs humaines diminuent et le travail devient plus fiable.* ».

5. Discussion des résultats

Les résultats de cette étude confirment que dans le secteur bancaire marocain, la GRH n'est pas une fonction support, c'est un dispositif central de maîtrise du risque opérationnel. Ce

constat, cohérent avec les travaux de Ferrary (2009) et la Resource-Based View (Barney, 1991), traverse l'ensemble des entretiens et structure les développements qui suivent.

5.1. Le rôle stratégique de la fonction RH : Confirmation de H1

Les répondants sont unanimes sur ce point. Recrutement rigoureux, formation continue, sensibilisation des collaborateurs : ce sont les premiers remparts contre le risque humain. Un directeur le formule clairement : *"La fonction RH contribue à la prévention du risque humain à travers un recrutement rigoureux, des plans de formation continue et des actions de sensibilisation, en coordination avec la direction risques et l'audit interne."*

Ce résultat rejoint Benlahcen Tlemcani & Amari (2020), qui montrent que les banques marocaines ayant formalisé leur politique RH présentent des niveaux d'incidents opérationnels significativement plus faibles. Il confirme aussi la thèse de Huselid (1995) sur l'impact des systèmes RH à haute performance sur la réduction des comportements à risque.

Ce qui est plus original dans nos résultats, c'est l'accent mis sur la coordination inter-directions RH, risques, audit interne comme condition de l'efficacité de ces pratiques. La plupart des travaux traitent la fonction RH de façon isolée. Nos données montrent que son efficacité dépend d'une articulation structurelle avec les autres fonctions de contrôle ce qui rejoint les développements de Weick & Sutcliffe (2001) sur la résilience organisationnelle.

5.2. Les profils stratégiques et la continuité d'activité : Confirmation de H2

Les répondants identifient sans hésiter les profils à risque élevé : directeurs d'agence, chargés de clientèle, traders, analystes risque, experts conformité. L'un d'eux est explicite : *"Les directeurs d'agences et les chargés de clientèle détiennent un portefeuille de clients importants qui pourrait impacter négativement l'activité et la performance de l'entreprise."*

Ce constat confirme empiriquement la thèse de Barney (1991) sur les ressources VRIN : ces profils sont rares, difficilement substituables à court terme, porteurs de savoirs tacites non codifiables. Leur départ ne représente pas un simple coût de remplacement c'est une perte d'avantage concurrentiel durable. Les mesures déployées en réponse, plans de relève, documentation des procédures, intérim, rémunération variable, correspondent aux mécanismes préconisés par la littérature sur la gestion des successions (Alias et al., 2016).

Un résultat inattendu mérite d'être signalé : la mention du médecin du travail comme acteur de prévention du risque humain. Ce rôle est peu documenté dans la littérature francophone sur le risque bancaire, il ouvre une piste de recherche intéressante sur le lien entre santé au travail et prévention des incidents opérationnels.

5.3. La fraude interne : Confirmation partielle de H2

Les postes les plus exposés à la fraude identifiée par les répondants gestion des comptes, analyse crédit, trésorerie correspondent exactement aux catégories à risque identifiées par le Comité de Bâle (2003) et confirmées empiriquement par Abdullahi & Mansor (2015). Les mesures déployées, contrôle interne strict, séparation des tâches, rotation des postes,

automatisation, s'inscrivent dans la logique de Jensen & Meckling (1976) : réduire les opportunités de fraude tout en augmentant les coûts des comportements déviants.

Mais un décalage est observable. Si les dispositifs formels sont bien en place, la culture éthique pourtant identifiée comme levier majeur par Khanna & Arora (2009), reste peu formalisée dans les discours. La prévention de la fraude est davantage vécue comme un exercice de contrôle que comme une démarche de construction de valeurs partagées. Ce décalage constitue une limite réelle des dispositifs actuels et une piste d'amélioration concrète pour les établissements marocains.

5.4. Les erreurs humaines : Confirmation de H1

Les facteurs d'erreur identifiés, stress, procédures complexes, supervision insuffisante, déficit de formation, défaillances systèmes, recourent le modèle systémique de Reason (1990) : les erreurs ne sont pas des faits isolés, elles résultent d'une combinaison de défaillances organisationnelles et individuelles. Les acteurs bancaires marocains ont visiblement intégré cette lecture systémique, les mesures proposées combinent formation, simplification des processus et amélioration des conditions de travail.

Un point mérite d'être relevé : les répondants insistent sur l'équité dans la gestion des promotions et évaluations comme facteur de réduction des erreurs. Ce lien peu exploré dans la littérature sur le risque opérationnel rejoint les travaux en psychologie organisationnelle sur le lien entre justice organisationnelle perçue et comportements de vigilance (cos et al., 2001). C'est une piste que les recherches futures gagneraient à approfondir.

5.5. La culture organisationnelle du risque : Confirmation de H3

Le résultat le plus transversal de cette étude est celui-ci : les pratiques RH n'opèrent efficacement que lorsqu'elles s'inscrivent dans une culture organisationnelle du risque construite collectivement entre la fonction RH, la direction des risques et l'audit interne. Aucune pratique isolée ne suffit, c'est leur cohérence systémique qui fait la différence.

Ce résultat valide H3 et rejoint Weick & Sutcliffe (2001) : la résilience ne se décrète pas par des procédures, elle se construit par une culture collective de vigilance et de responsabilité partagée. Dans le contexte marocain, bar (2024) reconnaît ce déficit de coordination inter-directions comme l'une des principales vulnérabilités structurelles du secteur ce qui donne à ce résultat une portée managériale directe.

Tableau 3 : Synthèse des résultats et validation des hypothèses

Hypothèse	Résultat terrain	Ancrage théorique	Statut
H1 : Formation et compétences réduisent le risque d'erreur	Confirmé : formation, procédures, automatisation	Reason (1990), Huselid (1995)	Validée ✓

H2 : Rémunération incitative limite fraude et turnover	Confirmé : Salaire variable, plans de relève, rotation	Jensen & Meckling (1976), Barney (1991)	Validée ✓
H3 : Coordination RH/risques/audit construit la culture du risque	Confirmé : coordination inter-directions systématiquement citée	Weick & Sutcliffe (2001)	Validée ✓

Conclusion

La présente étude souligne que le risque humain constitue un enjeu stratégique majeur dans le secteur bancaire marocain, où la performance repose fortement sur le capital humain. Sa maîtrise dépasse les seuls dispositifs réglementaires ou techniques et dépend étroitement de l'intégration des pratiques de gestion des ressources humaines à la gouvernance des établissements. La fonction RH contribue de manière significative à la prévention des risques via le recrutement, la formation continue, la gestion des compétences et la sensibilisation des collaborateurs, en coordination avec les directions risques et audit pour renforcer une culture organisationnelle du risque. Les profils à forte responsabilité, tels que ceux impliqués dans la gestion de la clientèle, la trésorerie ou la conformité, sont particulièrement exposés, justifiant la mise en œuvre de dispositifs anticipatifs comme les plans de relève, la formalisation des procédures et la formation ciblée. La combinaison de contrôles internes, de rotation des postes et d'automatisation contribue à réduire les opportunités de fraude, tandis que la communication et la formation permettent de limiter les erreurs humaines. La gestion du risque humain articulant pratiques RH, dispositifs de contrôle et culture organisationnelle apparaît ainsi comme un levier essentiel pour garantir la performance durable et la stabilité des banques marocaines.

- Apports théoriques

Sur le plan théorique, cet article apporte trois contributions à la littérature. Il propose d'abord une lecture intégrée du risque humain en articulant trois ancrages rarement mobilisés conjointement, la Resource-Based View (Barney, 1991), la théorie des incitations (Jensen & Meckling, 1976) et la résilience organisationnelle (Weick & Sutcliffe, 2001). Il enrichit ensuite les travaux de Ferrary (2009) en les confrontant à un terrain empirique marocain, confirmant la pertinence de ses typologies dans un contexte non occidental.

Il met enfin en évidence le rôle de la coordination inter-directions RH, risques, audit comme condition structurelle de l'efficacité des pratiques RH, un résultat peu documenté dans la littérature francophone sur le risque bancaire.

- Apports managériaux

Sur le plan managérial, trois recommandations concrètes se dégagent pour les établissements bancaires marocains. Premièrement, formaliser la coordination entre la fonction RH, la direction des risques et l'audit interne via des comités transversaux dédiés à la culture du risque. Deuxièmement, investir dans la cartographie des compétences stratégiques et dans des plans de succession opérationnels, pour anticiper les départs et préserver les savoir-faire critiques. Troisièmement et c'est peut-être le plus structurant, dépasser la logique du contrôle formel pour construire une culture éthique réelle, ancrée dans des programmes de formation aux valeurs et des dispositifs de reconnaissance de la performance responsable.

- Limites méthodologiques

Cette recherche comporte plusieurs limites méthodologiques. La première est structurelle : dix entretiens, c'est suffisant pour une démarche exploratoire, mais insuffisant pour généraliser les résultats à l'ensemble du secteur bancaire marocain. Les perceptions recueillies peuvent par ailleurs être influencées par des biais de désirabilité sociale les répondants décrivant parfois ce qui devrait être fait plutôt que ce qui est réellement pratiqué. La deuxième limite tient au périmètre géographique : les résultats sont contextualisés au Maroc et ne peuvent être transposés directement à d'autres systèmes bancaires sans précaution. Enfin, l'approche qualitative identifie et décrit les relations entre variables elle ne les quantifie pas.

- Perspectives de recherche futures

Ces limites ouvrent des pistes stimulantes. Une étude quantitative à grande échelle permettrait de tester statistiquement les relations entre pratiques RH et niveau de risque opérationnel, et d'en mesurer l'intensité réelle. Une étude comparative entre le Maroc et d'autres pays ayant transposé Bâle III permettrait d'évaluer l'influence du contexte réglementaire sur l'efficacité des pratiques RH. Enfin, le rôle de la santé au travail dans la prévention des incidents opérationnels signalé comme résultat inattendu dans cette étude mériterait d'être exploré plus systématiquement.

Bibliographie

Abdullahi, R., & Mansor, N. (2015). Fraud triangle theory and fraud diamond theory: Understanding the convergent and divergent for future research. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, 5(4), 54–64. <https://doi.org/10.6007/IJARAFMS/v5-i4/1823>

- Alias, N. E., Nor, N. M., & Hassan, R. (2016). The relationships between talent management practices, employee engagement, and employee retention in the IT organizations in Selangor. *Procedia Economics and Finance*, 35, 516–525.
- Bank Al-Maghrib. (2024). *Rapport annuel sur la supervision bancaire*. Bank Al-Maghrib.
- Barney, J. B. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, 17(1), 99–120.
- Basel Committee on Banking Supervision. (2003). *Sound practices for the management and supervision of operational risk*. Bank for International Settlements.
- Basel Committee on Banking Supervision. (2004). *International convergence of capital measurement and capital standards: A revised framework*. Bank for International Settlements. <https://www.bis.org/publ/bcbs107.htm>
- Basel Committee on Banking Supervision. (2017). *Basel III: Finalising post-crisis reforms*. Bank for International Settlements. <https://www.bis.org/bcbs/publ/d424.htm>
- Basel Committee on Banking Supervision. (2021). *Basel III monitoring report*. Bank for International Settlements.
- Becker, G. (1962). Investment in human capital: A theoretical analysis. *Journal of Political Economy*, 70(5), 9–49.
- Chernobai, A., Jorion, P., & Yu, F. (2011). The determinants of operational risk in U.S. financial institutions. *Journal of Financial and Quantitative Analysis*, 46(6), 1683–1725.
- Colquitt, J. A., Conlon, D. E., Wesson, M. J., Porter, C. O., & Ng, K. Y. (2001). Justice at the millennium: A meta-analytic review of 25 years of organizational justice research. *Journal of Applied Psychology*, 86(3), 425–445.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO). (1994). *Internal control – Integrated framework*. COSO.
- Crozier, M., & Friedberg, E. (1977). *L'acteur et le système : les contraintes de l'action collective*. Éditions du Seuil.
- Ferrary, M. (2009). Les ressources humaines à risque dans le secteur bancaire : une application de la gestion des risques opérationnels. *Gestion 2000*, 2, 85–102.
- HM Treasury. (2023). *The orange book: Management of risk – Principles and concepts*. HM Treasury.
- Hollnagel, E., Woods, D. D., & Leveson, N. (2006). *Resilience engineering: Concepts and precepts*. Ashgate Publishing.
- Huselid, M. A. (1995). The impact of human resource management practices on turnover, productivity, and corporate financial performance. *Academy of Management Journal*, 38(3), 635–672.
- Institute of Internal Auditors (IIA). (2004). *Enterprise risk management – Integrated framework*. Institute of Internal Auditors.

- Institute of Risk Management (IRM). (2010). *A structured approach to enterprise risk management and the requirements of ISO 31000*. IRM.
- Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305–360.
- Khanna, A., & Arora, B. (2009). A study to investigate the reasons for bank frauds and the implementation of preventive security controls in Indian banking industry. *International Journal of Business Science and Applied Management*, 4(3), 1–21.
- Penrose, E. T. (1959). *The theory of the growth of the firm*. Blackwell.
- Reason, J. (1990). *Human error*. Cambridge University Press.
- Thirlwell, J. (2010). Many-headed hydra: Operational risk is everywhere in your business so learn to manage it. *The Treasurer*, December.
- Timsit, D. (2010). *Gestion des risques opérationnels : théorie et pratique*. Economica.
- Weick, K. E., & Sutcliffe, K. M. (2001). *Managing the unexpected: Assuring high performance in an age of complexity*. Jossey-Bass.

CHAPTRE 11 : *Gestion des risques et performance des stratégies marketing omnicanales : proposition d'un modèle conceptuel dans un environnement incertain*

AHMAME Meryem

Docteure en Sciences Economiques et Gestion, FSJESO- Ahmamemeryem@yahoo.fr

Dans un contexte mondial marqué par des bouleversements économiques fréquents et une évolution technologique rapide, les entreprises se doivent d'adapter continuellement leurs stratégies marketing pour rester compétitives. Le marketing omnicanal, qui vise à offrir une expérience client fluide, cohérente et personnalisée à travers la multiplication des points de contact physiques et digitaux, représente aujourd'hui une approche incontournable (Verhoef, Kannan, & Inman, 2015). Pourtant, cette multiplication des canaux accroît la complexité opérationnelle et expose les organisations à une diversité accrue de risques, notamment liés à la sécurité des données, à la gestion des systèmes d'information, et à la volatilité des marchés (Ghantous, 2022).

Dans ce contexte incertain, la gestion proactive des risques apparaît comme un levier stratégique majeur permettant d'anticiper, d'évaluer et de réduire les impacts négatifs susceptibles de compromettre la performance des stratégies omnicanales. Toutefois, malgré la reconnaissance de cette importance, la littérature scientifique reste fragmentaire quant à l'interaction spécifique entre les pratiques de gestion des risques et les dimensions clés du marketing omnicanal telles que la cohérence des canaux, la personnalisation de l'offre, et la satisfaction client.

L'objectif principal de cet article est de contribuer à combler cette lacune par le biais d'une revue de littérature rigoureuse, synthétisant les travaux existants afin d'élaborer un modèle conceptuel intégrateur. Ce modèle vise à mieux comprendre comment la gestion des risques peut renforcer la résilience organisationnelle et optimiser la performance marketing dans un environnement caractérisé par une incertitude constante. En fournissant un cadre théorique enrichi, cette étude ambitionne également de proposer des pistes de réflexion pour les recherches futures et des orientations pratiques pour les managers.

La problématique spécifique abordée dans cet article est la suivante : comment la gestion proactive des risques influence-t-elle l'efficacité et la résilience des stratégies marketing omnicanales dans un environnement complexe et incertain ? Plus précisément, il s'agit d'examiner dans quelle mesure les pratiques de gestion des risques contribuent à la cohérence des canaux, à la personnalisation des offres et à la performance globale des dispositifs omnicanaux.

Cette recherche propose, à partir d'une revue documentaire rigoureuse, un modèle conceptuel intégrant ces aspects. L'objectif est de mieux comprendre comment la gestion des risques peut renforcer la résilience organisationnelle et optimiser la performance marketing dans un

environnement incertain. Cette recherche fournit un cadre théorique utile pour orienter les futures études et guider les pratiques managériales.

Le travail est structuré en quatre parties : revue de littérature, présentation du modèle conceptuel, discussion des implications, et conclusion avec recommandations.

1. Méthodologie de recherche

Cette recherche adopte une approche qualitative fondée sur une revue systématique de la littérature visant à analyser les relations entre la gestion des risques, la résilience organisationnelle et la performance des stratégies marketing omnicanales dans un environnement incertain.

La collecte des données bibliographiques a été réalisée à partir de plusieurs bases de données académiques reconnues, notamment Scopus, Web of Science, ScienceDirect et Google Scholar. Afin d'identifier les travaux les plus pertinents, plusieurs mots-clés ont été utilisés seuls ou en combinaison : « risk management », « omnichannel marketing », « marketing performance », « organizational resilience », « customer experience », « dynamic capabilities » et « organizational performance ».

Les publications sélectionnées couvrent principalement la période 2015-2025 afin de tenir compte des évolutions récentes liées à la transformation digitale et au développement des stratégies omnicanales. Les critères d'inclusion retenus concernent les articles scientifiques publiés dans des revues à comité de lecture, les ouvrages académiques de référence ainsi que les études empiriques portant sur la gestion des risques, le marketing omnicanal et la résilience organisationnelle. À l'inverse, les documents professionnels, les blogs, les rapports commerciaux et les sources ne présentant pas de validation scientifique ont été exclus de l'analyse.

Le processus de sélection s'est déroulé en plusieurs étapes. Dans un premier temps, une recherche documentaire a permis d'identifier un ensemble de publications potentiellement pertinentes. Dans un second temps, un examen des titres, résumés et mots-clés a été réalisé afin d'éliminer les travaux ne correspondant pas aux objectifs de la recherche. Enfin, les articles retenus ont fait l'objet d'une lecture approfondie permettant d'extraire les principaux concepts, variables et relations théoriques mobilisés dans la littérature.

L'analyse des travaux sélectionnés a été conduite selon une démarche de synthèse thématique visant à identifier les convergences et les complémentarités entre les différentes approches théoriques. Cette analyse a permis de construire un modèle conceptuel intégrateur mettant en relation la gestion des risques, la cohérence des stratégies omnicanales, la satisfaction client, la résilience organisationnelle et la performance marketing.

Cette démarche méthodologique vise à assurer la rigueur scientifique de la recherche tout en fournissant un cadre théorique cohérent susceptible de guider de futures investigations empiriques.

Tableau 1 : Synthèse des principaux articles mobilisés dans la revue de littérature

Auteur(s)	Année	Objectif de l'étude	Méthodologie	Principaux résultats
Verhoef, Kannan & Inman	2015	Analyser la transition du multicanal vers l'omnicanal	Revue conceptuelle	L'omnicanal améliore l'expérience client via l'intégration des canaux
Ghantous	2022	Étudier les stratégies omnicanales et la gestion des savoir-faire	Étude conceptuelle et exploratoire	La coordination des canaux est un facteur clé de performance
SafetyCulture	2025	Présenter les bonnes pratiques de gestion des risques	Analyse descriptive	La gestion proactive des risques améliore la continuité opérationnelle
Qualtrics	2025	Examiner la gestion des données client en omnicanal	Rapport analytique	Les données centralisées améliorent la personnalisation
Emarsys	2020	Étudier le rôle du marketing data-driven	Étude empirique	Les données clients renforcent la performance marketing
Salesforce	2023	Analyse des CDP et gestion des données clients	Étude de cas	Les plateformes CDP améliorent la connaissance client
Ringover	2024	Étudier la cohérence du parcours client omnicanal	Revue professionnelle	La cohérence améliore la satisfaction client
EdC Paris	2025	Étudier la transformation organisationnelle	Analyse conceptuelle	La collaboration interne est essentielle à l'omnicanal

2. Revue de littérature

Le marketing omnicanal, faisant référence à une approche intégrée utilisant simultanément et de manière interconnectée plusieurs canaux de communication, de vente et de relation client, vise à offrir une expérience unifiée et cohérente au consommateur, quel que soit le point de contact (Verhoef, Kannan, & Inman, 2015; Amazon Advertising, 2025). Cette stratégie permet de suivre le parcours client depuis la découverte de la marque jusqu'à l'achat et la fidélisation, tout en optimisant la personnalisation des offres et la fluidité des échanges à travers tous les canaux (Qualtrics, 2025). La multiplicité et la diversité des canaux exigent ainsi une coordination rigoureuse et une gestion efficace des données.

Parallèlement, la gestion des risques dans le marketing digital occupe une place fondamentale. Elle porte principalement sur l'identification et la mitigation des risques liés à la sécurité des données, à la réputation de la marque et à la performance technologique des systèmes mis en œuvre (Ghantous, 2022; SafetyCulture, 2025). Ces risques sont particulièrement critiques en contexte omnicanal, où une faille dans un seul canal peut affecter l'ensemble de l'expérience client et compromettre la fidélité des consommateurs.

Cependant, bien que ces domaines soient chacun bien documentés, il reste peu d'études approfondissant leur interaction, notamment comment la gestion proactive des risques peut influencer la cohérence des canaux et, par extension, la satisfaction et la fidélisation client. Ce manque justifie la construction d'un modèle conceptuel qui examine ces interdépendances et met en lumière le rôle médiateur de la gestion des risques dans l'efficacité globale des stratégies omnicanales.

3.1 Fondements théoriques de la recherche

L'analyse de l'impact de la gestion des risques sur les stratégies marketing omnicanales peut être appréhendée à travers plusieurs cadres théoriques complémentaires permettant d'expliquer les mécanismes par lesquels les organisations développent leur capacité d'adaptation et améliorent leur performance dans des environnements incertains.

3.1.1 La théorie des ressources et compétences (Resource-Based View)

La théorie des ressources et compétences (Resource-Based View - RBV), développée notamment par Barney (1991), considère que l'avantage concurrentiel durable d'une entreprise

repose sur la possession et la mobilisation efficace de ressources rares, précieuses, difficilement imitables et non substituables. Dans cette perspective, la gestion des risques peut être considérée comme une capacité organisationnelle stratégique permettant à l'entreprise de protéger ses ressources critiques, d'anticiper les menaces et de maintenir sa performance face aux perturbations de l'environnement.

Dans le contexte du marketing omnicanal, la maîtrise des risques liés aux technologies, aux données clients et à la coordination des différents canaux constitue une ressource stratégique contribuant à la création de valeur. Une gestion efficace des risques permet ainsi de renforcer la confiance des clients, de sécuriser les processus organisationnels et de soutenir un avantage concurrentiel durable.

3.1.2. La théorie des capacités dynamiques (Dynamic Capabilities Theory)

La théorie des capacités dynamiques, proposée par Teece, Pisano et Shuen (1997), met l'accent sur l'aptitude des entreprises à intégrer, développer et reconfigurer leurs ressources afin de répondre aux évolutions rapides de leur environnement. Selon cette approche, les organisations performantes sont celles qui parviennent à détecter les changements, à saisir les opportunités et à transformer leurs ressources de manière continue.

L'environnement omnicanal est caractérisé par une forte évolution technologique, des attentes clients changeantes et une concurrence accrue. Dans ce contexte, la gestion des risques constitue une capacité dynamique essentielle permettant aux entreprises d'identifier rapidement les menaces émergentes, d'adapter leurs processus et de préserver la continuité de leurs activités. Elle favorise également la résilience organisationnelle en permettant une meilleure adaptation aux situations d'incertitude.

3.1.3. La théorie de la contingence (Contingency Theory)

La théorie de la contingence soutient qu'il n'existe pas de modèle de gestion universellement efficace et que la performance organisationnelle dépend de l'adéquation entre les caractéristiques de l'entreprise et les conditions de son environnement (Donaldson, 2001). Cette approche est particulièrement pertinente pour comprendre la relation entre la gestion des risques et les stratégies marketing omnicanales.

En effet, l'efficacité des dispositifs omnicanaux varie selon plusieurs facteurs contingents tels que la taille de l'entreprise, son secteur d'activité, son niveau de digitalisation ou encore le degré d'incertitude de son environnement. Dès lors, les pratiques de gestion des risques doivent être adaptées aux spécificités de chaque organisation afin d'assurer une meilleure cohérence entre les canaux, une expérience client homogène et une performance marketing optimale.

3.1.4. Synthèse du cadre théorique

L'articulation de ces trois approches théoriques permet de construire un cadre d'analyse cohérent pour étudier l'impact de la gestion des risques sur les stratégies marketing omnicanales. La théorie des ressources et compétences explique le rôle stratégique de la gestion des risques comme source d'avantage concurrentiel. La théorie des capacités dynamiques met en évidence son importance dans l'adaptation aux changements et le développement de la résilience organisationnelle. Enfin, la théorie de la contingence souligne la nécessité d'adapter les pratiques de gestion aux caractéristiques spécifiques de l'environnement.

Ces fondements théoriques justifient la proposition d'un modèle conceptuel dans lequel la gestion des risques agit comme un facteur déterminant de la résilience organisationnelle, de la cohérence omnicanale et, in fine, de la performance marketing.

3.2 Modèle conceptuel

Le marketing omnicanal vise à créer une expérience client fluide et intégrée en connectant l'ensemble des points de contact physiques et digitaux, permettant au consommateur de naviguer sans heurts entre les canaux (Verhoef, Kannan, & Inman, 2015). Pour atteindre cette cohérence, il est essentiel que les entreprises analysent précisément les parcours clients, identifient les moments clés d'interaction, et intègrent les données issues de tous les canaux afin de proposer des offres personnalisées et pertinentes (Ringover, 2024).

Cependant, en lien avec cette complexité, la gestion des risques joue un rôle central. Elle consiste en l'identification, l'évaluation et la mitigation des menaces pouvant affecter la sécurité des données, la qualité des systèmes d'information, ou encore la réputation de la marque (Ghantous, 2022; SafetyCulture, 2025). Dans un environnement incertain, une gestion proactive des risques assure la continuité des opérations et protège l'intégrité de l'expérience omnicanale.

Le modèle conceptuel proposé dans cet article articule donc trois dimensions principales :

La gestion des risques, incluant les mécanismes d'anticipation et de réduction des risques technologiques et commerciaux.

La cohérence des canaux omnicanaux, caractérisée par une expérience uniforme, une intégration des données et une personnalisation adaptée.

La performance marketing, mesurée par la satisfaction client, la fidélisation et l'efficacité commerciale.

Gestion des risques

(Identification - Evaluation - Mitigation)



Cohérence des stratégies omnicanales

(Intégration technologique -

Personnalisation -

Cohérence des canaux)



Satisfaction client



Performance marketing

(Fidélisation -

Performance commerciale -

Avantage concurrentiel)

Résilience organisationnelle

(Médiateur)

P4

Gestion des risques —► Performance marketing

Figure 1. Modèle conceptuel proposé de l'impact de la gestion des risques sur la performance des stratégies marketing omnicanales dans un environnement incertain.

P1 : Gestion des risques → Cohérence omnicanale

P2 : Cohérence omnicanale → Satisfaction client

P3 : Satisfaction client → Performance marketing

P4 : Résilience organisationnelle médiatise la relation entre gestion des risques et performance marketing.

4. Propositions de recherche

À partir de la revue de littérature et des fondements théoriques mobilisés, plusieurs propositions de recherche peuvent être formulées afin d'explicitier les relations entre la gestion des risques, la résilience organisationnelle, la cohérence omnicanale et la performance marketing.

Proposition 1 : Effet de la gestion des risques sur la cohérence omnicanale

La littérature souligne que les stratégies omnicanales reposent sur une intégration efficace des technologies, des données et des processus organisationnels. Une gestion proactive des risques permet d'anticiper les défaillances techniques, les risques liés aux données ainsi que les perturbations organisationnelles susceptibles d'affecter l'expérience client. En réduisant ces vulnérabilités, les entreprises sont davantage en mesure d'assurer la cohérence et la continuité entre les différents canaux de communication et de distribution.

P1 : La gestion proactive des risques influence positivement la cohérence des stratégies marketing omnicanales.

Proposition 2 : Effet de la cohérence omnicanale sur la satisfaction client

L'un des objectifs fondamentaux de l'approche omnicanale consiste à offrir au consommateur une expérience fluide, homogène et personnalisée tout au long de son parcours. Lorsque les différents canaux sont intégrés et cohérents, les clients bénéficient d'une meilleure qualité de service, d'une réduction des frictions et d'une expérience plus satisfaisante.

P2 : La cohérence des stratégies marketing omnicanales influence positivement la satisfaction client.

Proposition 3 : Effet de la satisfaction client sur la performance marketing

De nombreux travaux démontrent que la satisfaction client constitue un déterminant majeur de la fidélisation, de l'intention de réachat et du bouche-à-oreille positif. Dans le cadre des stratégies omnicanales, une expérience satisfaisante contribue à renforcer la relation entre l'entreprise et ses clients, ce qui se traduit par une amélioration de la performance marketing et commerciale.

P3 : La satisfaction client influence positivement la performance marketing.

Proposition 4 : Rôle médiateur de la résilience organisationnelle

Face à l'incertitude économique et technologique, la résilience organisationnelle représente la capacité de l'entreprise à anticiper, absorber et surmonter les perturbations. La gestion des risques contribue au développement de cette capacité adaptative, laquelle favorise à son tour le maintien de la performance marketing malgré les changements de l'environnement. La résilience apparaît ainsi comme un mécanisme explicatif essentiel reliant la gestion des risques à la performance organisationnelle.

P4 : La résilience organisationnelle joue un rôle médiateur dans la relation entre la gestion des risques et la performance marketing.

Synthèse des propositions

Le modèle conceptuel proposé suggère que la gestion proactive des risques agit comme un levier stratégique permettant de renforcer la résilience organisationnelle et la cohérence omnicanale. Ces facteurs favorisent ensuite la satisfaction client, laquelle contribue à l'amélioration de la performance marketing. L'ensemble de ces relations constitue un cadre théorique pouvant faire l'objet d'une validation empirique dans de futures recherches.

Les principaux défis de l'intégration omnicanale pour les entreprises

Les principaux défis de l'intégration omnicanale pour les entreprises sont les suivants :

Intégration technologique complexe : Assurer la cohérence et la communication fluide entre les différentes plateformes digitales et points de vente physiques nécessite des systèmes d'information sophistiqués et bien connectés, ce qui peut représenter un défi technique majeur.

L'intégration technologique dans les stratégies omnicanales constitue un défi majeur pour les entreprises en raison de la nécessité d'assurer une communication fluide et cohérente entre des plateformes digitales multiples et les points de vente physiques. Cela requiert des systèmes d'information à la fois sophistiqués et parfaitement interconnectés, capables de synchroniser les données et les processus en temps réel. Ce niveau d'intégration est indispensable pour garantir une expérience client homogène, mais il s'accompagne de défis techniques considérables, notamment en matière de gestion des flux d'informations, d'interopérabilité des technologies et de maintien de la sécurité des données (Verhoef, Kannan, & Inman, 2015; Ghantous, 2022).

Selon la littérature académique, l'un des obstacles principaux à cette intégration réside dans la fragmentation des systèmes d'information au sein des entreprises, souvent cloisonnés par fonctions ou par canaux, ce qui complique la création d'un parcours client unifié et sans rupture (Bernard, 2024; Franchise-FFF, 2023). Pour pallier cette complexité, il est nécessaire de mettre en œuvre des architectures technologiques flexibles et évolutives, intégrant des solutions CRM, ERP et des plateformes analytiques qui centralisent et consolident les données clients (Qualtrics, 2025).

De plus, l'intégration omnicanale exige une coordination approfondie entre les équipes marketing, logistique, informatique, et relation client. Cette coordination nécessite non seulement des outils technologiques adaptés mais aussi une transformation organisationnelle et culturelle pour briser les silos internes (EdC Paris, 2025). La capacité à gérer efficacement ces aspects techniques est un facteur clé de succès, directement liée à la qualité de l'expérience client et à la performance marketing globale (SafetyCulture, 2025).

Gestion des données : Collecter, centraliser, analyser et sécuriser les données clients provenant de multiples canaux est essentiel pour offrir une expérience personnalisée, mais la diversité et le volume des données rendent cette tâche ardue.

La gestion des données dans une stratégie marketing omnicanale constitue un défi majeur pour les entreprises. Elle implique de collecter, centraliser, analyser et sécuriser des volumes importants de données clients issus de multiples canaux tels que les magasins physiques, le e-commerce, les réseaux sociaux, les applications mobiles et les points de contact directs (Verhoef, Kannan, & Inman, 2015; Qualtrics, 2025). Cette diversité rend la gestion complexe car les données sont souvent fragmentées et stockées dans des silos techniques distincts,

empêchant une vision client unifiée et une personnalisation efficace des offres (Ghantous, 2022; Emarsys, 2020).

Pour pallier ces difficultés, de nombreuses entreprises investissent dans des plateformes centralisées, telles que les Customer Data Platforms (CDP), qui agrègent, nettoient et analysent en temps réel les données issues de différents canaux afin de créer des profils clients complets et dynamiques (SafetyCulture, 2025; Salesforce, 2023). Ces outils permettent de mieux comprendre les comportements des consommateurs et d'adapter les communications et offres en conséquence.

Cependant, cette gestion massive de données soulève également des enjeux majeurs en matière de sécurité, confidentialité et conformité aux réglementations telles que le RGPD. La protection des données sensibles et la construction de la confiance client deviennent ainsi des priorités absolues (Ghantous, 2022; SafetyCulture, 2025).

Cohérence et homogénéité de l'expérience client : Garantir que le consommateur vive une expérience fluide, sans rupture ni incohérence entre les canaux physiques et digitaux, reste un défi crucial car des écarts peuvent nuire à la satisfaction et à la fidélité.

Cohérence et homogénéité de l'expérience client

Garantir une expérience fluide et homogène pour le client, quels que soient le canal ou le point de contact, constitue un défi central dans la stratégie omnicanale (Vocalcom, 2024). La cohérence ne se limite pas à la simple uniformité de la communication ou de l'apparence visuelle, mais englobe également la continuité de l'expérience, la reconnaissance du client, et la qualité de service à chaque étape de son parcours (ChapsVision, 2025).

L'un des enjeux majeurs est la cartographie précise du parcours client, qui nécessite de recenser tous les points de contact, que ce soit en ligne, via une application mobile, en magasin ou par téléphone. Ce processus permet d'identifier les écarts, les points de friction, et les opportunités d'amélioration, afin d'assurer une transition sans rupture entre les canaux (LinkMobility, 2024). La synchronisation des données est essentielle pour que chaque interaction soit contextualisée et que le client retrouve ses informations et préférences, quelle que soit la modalité ou le support utilisé.

La cohérence de l'expérience implique également un alignement des équipes en interne. La collaboration interservices, la formation et la mise en œuvre d'outils technologiques communs sont nécessaires pour que chaque contact avec le client reflète une identité de marque cohérente,

un ton uniforme, et une qualité de service irréprochable (EdC Paris, 2025). Enfin, la gestion de l'expérience client doit s'appuyer sur des indicateurs précis et réguliers, pour ajuster en permanence la stratégie et corriger les écarts, mais aussi pour renforcer la fidélité par une relation de confiance et de satisfaction durable.

Adaptation organisationnelle : Les entreprises doivent souvent revoir leurs processus internes et former leurs équipes pour fonctionner dans un mode omnicanal, ce qui implique un changement culturel et opérationnel important.

L'adaptation organisationnelle représente un défi majeur dans la mise en œuvre d'une stratégie omnicanale. Elle nécessite souvent une refonte profonde des processus internes et une transformation culturelle au sein de l'entreprise (Viseo, 2025). Les silos traditionnels entre les départements marketing, vente, service client et informatique doivent être brisés pour permettre une collaboration fluide et une vision unifiée centrée sur le client (Thilez Informatique, 2024).

Cette transformation inclut la redéfinition des rôles, la formation des équipes aux nouveaux outils et pratiques liés à l'omnicanal, ainsi que l'adoption d'une culture orientée vers l'expérience client cohérente et personnalisée sur tous les canaux (Viseo, 2025; Wikipédia, 2016). Le management doit impulser un leadership fort et clair afin d'accompagner ce changement organisationnel et éviter les résistances internes. L'adoption de nouvelles méthodes de travail, telles que l'agilité et la co-création entre départements, contribue également à une meilleure intégration omnicanale.

Par ailleurs, l'harmonisation des objectifs et des incitations entre les équipes est cruciale pour éviter les conflits d'intérêts, par exemple entre les ventes en ligne et en boutique, et garantir une approche réellement intégrée (EdC Paris, 2025).

Sécurité et gestion des risques : La multiplicité des points de contact expose les entreprises à des risques accrus liés à la sécurité des données, à la protection de la vie privée, et aux fraudes, nécessitant une gestion proactive des risques.

Risques sécuritaires et gestion des risques dans une stratégie omnicanale

La multiplication des points de contact dans une stratégie omnicanale augmente considérablement la surface d'attaque pour les cyberattaques et autres menaces liées à la sécurité des données (Relation-Client-Prodirect, 2025). Le risque principal réside dans la vulnérabilité accrue des systèmes d'information, notamment en ce qui concerne le vol de données, l'usurpation d'identité et la violation de la confidentialité (Web source, 2025). Ces incidents

peuvent entraîner des pertes financières, un déclin de la confiance client et des sanctions réglementaires, notamment avec la mise en œuvre de réglementations strictes telles que le RGPD (Cybersecurity & Data Protection, 2025).

Pour faire face à ces risques, il est essentiel d'adopter une gestion proactive renforcée par des mesures de sécurité robustes : chiffrement des données, authentification multi-facteur, surveillance en temps réel des flux de données, et formation continue du personnel (Widem, 2025; Web source, 2023). La sécurisation des échanges entre canaux doit également respecter les normes réglementaires et les meilleures pratiques en cybersécurité, réduisant ainsi le risque de violations et d'usurpation d'identité (MyStudies, 2023).

Le maintien d'une infrastructure technologique sécurisée est donc une condition indispensable pour préserver la confiance des clients et assurer la pérennité de la stratégie omnicanale. La gestion du risque doit inclure une évaluation régulière des vulnérabilités, la mise en place de protocoles d'intervention rapide, et une vigilance constante face aux nouvelles formes de cybermenaces (Sia Partners, 2023).

Coût et retour sur investissement : Mettre en place et maintenir une stratégie omnicanale demande des investissements significatifs en technologie, formation et gestion opérationnelle, avec un besoin constant d'évaluer la performance pour assurer une rentabilité.

Mettre en place et maintenir une stratégie omnicanale représente un investissement financier important et continu pour les entreprises. Les coûts englobent plusieurs volets, notamment l'acquisition et la mise à jour des technologies nécessaires pour gérer et synchroniser les multiples canaux physiques et digitaux (Antoine Blot, 2025 ; EdC Paris, 2025). Cela comprend l'achat ou le développement de systèmes CRM, plateformes de données clients, solutions d'automatisation et infrastructures IT évolutives capables d'assurer l'intégration en temps réel des informations clients.

Par ailleurs, les dépenses liées à la formation des équipes pour maîtriser ces nouveaux outils et adapter les processus internes sont non négligeables. Cette formation porte sur des pratiques omnicanales spécifiques, la gestion de la relation client multicanal, ainsi que sur la sensibilisation à la sécurité des données (Viseo, 2025; Antoine Blot, 2025).

Le retour sur investissement (ROI) doit être contrôlé régulièrement grâce à des indicateurs clés de performance (KPI) mesurant à la fois l'impact commercial (augmentation des ventes,

fidélisation) et la satisfaction client (cohérence de l'expérience, personnalisation) (Antoine Blot, 2025).

Conclusion

L'objectif de cet article était d'analyser le rôle de la gestion des risques dans l'amélioration de la performance des stratégies marketing omnicanales au sein d'un environnement caractérisé par une forte incertitude économique, technologique et concurrentielle. À travers une revue systématique de la littérature, cette recherche a mis en évidence que la multiplication des canaux de communication et de distribution, bien qu'elle représente une opportunité majeure pour renforcer l'expérience client, expose également les entreprises à de nombreux risques liés à la sécurité des données, à l'intégration technologique, à la coordination organisationnelle et à la volatilité de l'environnement.

L'analyse des travaux académiques mobilisés montre que la gestion proactive des risques constitue un levier stratégique essentiel pour assurer la continuité des activités, préserver la confiance des clients et améliorer l'efficacité des dispositifs omnicanaux. Les pratiques d'identification, d'évaluation et de maîtrise des risques permettent notamment de réduire les vulnérabilités opérationnelles, de renforcer la cohérence entre les différents canaux et de favoriser une meilleure qualité de l'expérience client.

Cette recherche contribue également à la littérature en proposant un modèle conceptuel intégrateur reliant la gestion des risques, la résilience organisationnelle, la cohérence omnicanale et la performance marketing. Ce modèle met en évidence le rôle central de la résilience organisationnelle comme mécanisme permettant aux entreprises de s'adapter aux perturbations et de maintenir leur performance dans des environnements complexes et changeants. Ainsi, la gestion des risques ne doit plus être considérée uniquement comme une fonction de protection, mais comme une capacité stratégique créatrice de valeur et de différenciation concurrentielle.

Sur le plan théorique, cette étude enrichit les travaux portant sur le marketing omnicanal en mobilisant plusieurs perspectives complémentaires, notamment la théorie des ressources et compétences (Resource-Based View), la théorie des capacités dynamiques (Dynamic Capabilities Theory) et la théorie de la contingence (Contingency Theory). Ces approches permettent de mieux comprendre comment les entreprises peuvent développer des capacités

organisationnelles favorisant l'adaptation, l'innovation et la performance dans un contexte d'incertitude croissante.

Sur le plan managérial, les résultats soulignent l'importance pour les décideurs d'intégrer la gestion des risques dès la conception des stratégies omnicanales. Les entreprises sont appelées à investir dans des infrastructures technologiques sécurisées, à renforcer les mécanismes de gouvernance des données, à développer une culture organisationnelle orientée vers la prévention des risques et à promouvoir une collaboration transversale entre les différentes fonctions de l'organisation. Une telle démarche contribue non seulement à réduire les risques potentiels, mais également à améliorer la satisfaction, la fidélisation et la confiance des clients.

Cependant, cette recherche présente certaines limites. Premièrement, elle repose exclusivement sur une analyse documentaire et ne comporte aucune validation empirique du modèle conceptuel proposé. Deuxièmement, les relations identifiées entre les variables sont fondées sur des résultats issus de contextes sectoriels et géographiques variés, ce qui peut limiter la généralisation des conclusions. Troisièmement, l'évolution rapide des technologies numériques et des comportements des consommateurs nécessite une actualisation continue des connaissances relatives aux stratégies omnicanales et à la gestion des risques.

Dans cette perspective, plusieurs pistes de recherche futures peuvent être envisagées. Il serait pertinent de procéder à une validation empirique du modèle conceptuel auprès d'entreprises ayant adopté une stratégie omnicanale, notamment à travers une approche quantitative fondée sur la modélisation par équations structurelles (SEM ou PLS-SEM). Des études comparatives entre différents secteurs d'activité ou entre pays développés et émergents permettraient également d'identifier les facteurs contextuels susceptibles d'influencer les relations observées. Enfin, l'exploration de nouvelles dimensions telles que l'intelligence artificielle, la cybersécurité, le Big Data ou encore la confiance numérique pourrait enrichir davantage la compréhension du rôle de la gestion des risques dans la performance des stratégies marketing omnicanales.

En définitive, dans un environnement marqué par l'incertitude et la transformation digitale permanente, la capacité des organisations à intégrer efficacement la gestion des risques dans leurs stratégies omnicanales apparaît comme une condition essentielle de leur résilience, de leur compétitivité et de leur performance durable.

Références

- Creswell, J. W., & Plano Clark, V. L. (2017). *Designing and Conducting Mixed Methods Research* (3rd ed.). SAGE Publications.
- Donaldson, L. (2001). *The Contingency Theory of Organizations*. Sage Publications.
- Ghantous, N. (2022). Stratégies omnicanales, marque, et gestion des savoir-faire en France. *Franchise Magazine*, 55, 34-89.
- Khatr, A., & Alaoui, M. (2024). Contribution de la big data à la réussite d'une stratégie marketing omnicanale dans le secteur bancaire marocain. *International Journal of Marketing and Strategic Management*, 6(1-2), 5-23. <https://doi.org/10.1016/j.jretai.2015.02.005>
- SafetyCulture. (2025). Gestion et analyse des risques : exemples et bonnes pratiques. Récupéré de <https://www.safetyculture.com/fr/themes/analyse-des-risques>
- Teece, D. J., Pisano, G., & Shuen, A. (1997). *Dynamic Capabilities and Strategic Management*. *Strategic Management Journal*, 18(7), 509-533.
- Verhoef, P. C., Kannan, P. K., & Inman, J. J. (2015). From Multi-channel Retailing to Omni-channel Retailing. *Journal of Retailing*, 91(2), 174–181.
- Verhoef, P. C., Kannan, P. K., & Inman, J. J. (2015). From Multi-channel Retailing to Omni-channel Retailing. *Journal of Retailing*, 91(2), 174–181. <https://doi.org/10.1016/j.jretai.2015.02.005>
- Barney, J. (1991). *Firm Resources and Sustained Competitive Advantage*. *Journal of Management*, 17(1), 99-120.

**CHAPITRE 12 : *Exploiter la transformation digitale pour rationaliser le
Système de Management de la Qualité (SMQ) dans les PME : entre
opportunités et risques numériques***

Imane BOUZEGGAOUI

Doctorante ,Equipe de Recherche EMAG , ENCGO, UMP,-Oujda-
imane.bouzeggaoui.1.24@ump.ac.ma

Majda ALAOUI

Enseignante-Chercheuse, Equipe de EMAG, ENCGO, UMP,-Oujda-
. m.alaoui@ump.ac.ma

Digitaliser la démarche qualité pour une PME revêt aujourd'hui une double face : un accélérateur de compétitivité autant qu'une nouvelle source de vulnérabilité. C'est cette tension, rarement traitée de façon intégrée, qui fonde le présent chapitre. La qualité devient un enjeu de compétitivité d'autant plus critique que les entreprises opèrent dans des environnements instables, fortement numérisés et soumis à des exigences croissantes de traçabilité. Pour les petites et moyennes entreprises (PME), cette pression est paradoxale : elles doivent démontrer la maîtrise de leurs processus tout en composant avec des ressources financières, humaines et technologiques plus limitées que celles des grandes organisations (Li et al., 2018 ; Matt & Rauch, 2020).

Dans ce contexte, le système de management de la qualité (SMQ), notamment lorsqu'il s'inspire de la norme ISO 9001:2015, offre un cadre structurant pour formaliser les processus, maîtriser les non-conformités et soutenir l'amélioration continue (Heras-Saizarbitoria & Boiral, 2013 ; Sampaio et al., 2009). La transformation digitale peut renforcer ce cadre en automatisant les tâches répétitives, en améliorant la disponibilité des données qualité et en accélérant les boucles de décision (Vial, 2019 ; Verhoef et al., 2021). Cependant, cette convergence suscite également des interrogations quant aux risques numériques qu'elle génère – cybermenaces, violations de données, vulnérabilités organisationnelles – susceptibles de compromettre l'intégrité même des systèmes qualité (Kshetri, 2021; Haque et al., 2025). Les PME, en raison de leurs contraintes structurelles spécifiques (ressources limitées, déficit de compétences numériques, charge opérationnelle élevée), se trouvent ainsi à la croisée de ces opportunités et de ces risques (Li et al., 2018; Goerzig & Bauernhansl, 2018).

Cette tension entre opportunités et risques soulève une problématique centrale : *dans quel mesure les PME peuvent-elles exploiter efficacement la transformation digitale pour rationaliser la mise en œuvre de leurs SMQ tout en atténuant les risques numériques associés ?* Cette question interpelle les chercheurs et les praticiens, d'autant que la littérature existante sur la transformation digitale demeure fragmentée, majoritairement orientée vers les grandes entreprises et focalisée sur des technologies spécifiques, sans proposer de cadre holistique adapté aux réalités des PME (Ghosh et al., 2022 ; Kohli & Melville, 2019).

L'objectif de cet article est de combler cette lacune en proposant une lecture intégrée de l'articulation entre transformation digitale, SMQ et risques numériques dans les PME. Plus précisément, il vise à : (1) clarifier les dimensions conceptuelles de la transformation digitale ; (2) identifier les mécanismes par lesquels les technologies numériques rationalisent les processus du SMQ ; (3) hiérarchiser les risques numériques associés à la digitalisation des SMQ selon leur criticité ; et (4) formaliser un modèle conceptuel intégrateur mobilisable pour de futures recherches empiriques.

Pour atteindre ces objectifs, une revue systématisée et intégrative de la littérature a été menée selon une démarche rigoureuse inspirée des protocoles de Torraco (2005) et Snyder (2019). Ce choix méthodologique se justifie par la nature encore émergente et fragmentée du champ de recherche, qui requiert une synthèse structurante plutôt qu'une agrégation statistique des résultats empiriques. Ainsi, la méthodologie retenue combine une analyse critique des travaux

académiques en management de la qualité, transformation digitale des PME, systèmes ISO 9001, Qualité 4.0 et gouvernance des risques numériques. La démarche ne vise pas une méta-analyse statistique, mais une synthèse conceptuelle à visée théorique.

Le corpus a été constitué à partir des bases de données académiques de référence (Scopus, Web of Science, Google Scholar) et complété par les actes des conférences spécialisées en management de la qualité numérique. La recherche a combiné des mots-clés relatifs aux quatre champs mobilisés. Les travaux ont été retenus selon leur pertinence thématique, leur qualité académique et leur contribution à la compréhension d'au moins l'un de ces champs ; les publications strictement techniques ou sans lien avec le contexte organisationnel des PME ont été écartées. L'analyse s'appuie sur une grille de lecture à quatre catégories – leviers digitaux, processus du SMQ, risques numériques et effets organisationnels – appliquée de manière transversale à l'ensemble du corpus. Cette grille a guidé l'extraction et la mise en relation des apports de chaque travail, puis leur synthèse thématique.

Le chapitre est structuré en trois sections principales pour une analyse approfondie et progressive : une conceptualisation de la transformation digitale, une revue de littérature critique et structurée, et la présentation d'un modèle conceptuel intégrateur.

1. Comprendre la transformation digitale : un essai de conceptualisation

La transformation digitale (TD) s'est imposée comme une réalité omniprésente dans la vie quotidienne et professionnelle, accélérée notamment par la pandémie de COVID-19 qui a généralisé le recours aux applications mobiles, services bancaires en ligne, e-commerce, enseignement à distance, télétravail et visioconférences. Son évolution historique peut être retracée depuis les années 1980, marquées par le développement de la micro-informatique et des architectures client/serveur, suivies dans les années 1990 et 2000 par l'émergence du Web et la maîtrise des flux de données numériques (Wiersh & Autissier, 2016). Progressivement, le digital s'est affirmé comme une technologie mobile générant de nouvelles pratiques et masses de données à traiter, tandis que la distinction entre « numérique » (informatisation et automatisation des données) et « digital » (technologies mobiles et supports) reste parfois floue.

Verhoef et al. (2021) proposent une conceptualisation en trois phases progressives et interdépendantes : la numérisation (conversion des données analogiques en format numérique), la digitalisation (utilisation des technologies numériques pour modifier les processus existants) (Li et al., 2018), et enfin la transformation digitale proprement dite, qui désigne un changement systémique et profond à l'échelle de l'entreprise, restructurant les modèles d'affaires, les processus, les relations avec les parties prenantes et, à terme, les économies et la société (Rachinger et al., 2018). Besson et al. (2017) la définissent comme la combinaison de l'automatisation, de la dématérialisation et de la réorganisation des intermédiations, touchant l'ensemble des activités de l'entreprise. Dans une contribution plus récente, Vial (2019) précise que ce processus repose sur les technologies SMACIT (Social, Mobile, Analytics, Cloud, Internet des objets) et sur l'émergence d'écosystèmes de plateformes, favorisant la collecte massive de données, leur traitement analytique (via algorithmes d'intelligence

artificielle notamment) et leur sécurisation, tout en s'appuyant sur des infrastructures web propices aux effets de réseau.

Aujourd'hui, la TD s'inscrit dans un environnement sociotechnique favorable à sa mise en œuvre : technologies accessibles, effets organisationnels et managériaux relativement prévisibles, légitimité du changement renforcée par la pandémie (Varenne & Godé, 2023). Elle redéfinit structures, flux de travail et modèles d'affaires grâce à l'exploitation de l'IoT, de l'IA et du big data pour accroître l'efficacité opérationnelle et la qualité décisionnelle (Prokhin, 2020).

Malgré une littérature abondante et en expansion (Kraus et al., 2022 ; Schallmo et al., 2019), aucune définition consensuelle n'émerge encore du terme « transformation digitale ». Les définitions recensées varient selon qu'elles insistent sur l'adoption technologique, l'amélioration des processus et des performances, la création de nouveaux modèles d'affaires ou les impacts systémiques sur les acteurs et environnements. Le tableau 1 synthétise cette hétérogénéité définitionnelle.

Tableau 1 : Synthèse des différentes définitions de la transformation digitale

Axe	Auteurs	Définition synthétique
Changement organisationnel	Liu, Chen & Chou (2011) ; Parviainen et al. (2017)	Processus de changement organisationnel rendu possible par l'intégration des technologies numériques, transformant pratiques de travail, rôles et activités.
Performance	Fitzgerald et al. (2013) ; Westerman et al. (2014)	Usage des technologies numériques pour obtenir des améliorations significatives des performances, de l'efficacité et/ou de la portée des activités.
Stratégie et valeur	Bharadwaj et al. (2013) ; Matt et al. (2015)	Démarche stratégique mobilisant des ressources numériques pour créer de la valeur et piloter les transformations induites dans l'organisation.
Business model	Hess et al. (2020) ; Warner & Wäger (2019)	Renouvellement (continu) des capacités et du business model, ainsi que des dimensions collaboratives/culturelles, grâce aux technologies numériques.
Écosystèmes	Hinings, Gegenhuber & Greenwood (2018) ;	Reconfiguration des réseaux d'acteurs (entreprise, clients, partenaires) et de la chaîne de valeur via technologies et données, avec de nouvelles formes d'interaction/coordination.

Axe	Auteurs	Définition synthétique
	Schallmo et al. (2019)	
Technologies numériques et connectivité	Vial (2019)	La digitalisation est un processus visant à améliorer une entité en provoquant des changements significatifs dans ses caractéristiques grâce à la fusion des technologies de l'information, de l'informatique, de la communication et de la connectivité.
Qualité et durabilité	Wang & Yan (2023)	La TD diffuse à grande échelle l'usage des technologies numériques pour soutenir une qualité « supérieure », alignée sur des objectifs organisationnels durables.

Source : élaboré par les auteurs

La digitalisation et la transformation digitale renvoient finalement au même phénomène fondamental : la création d'un environnement numérique unifié par la combinaison d'outils et de techniques de gestion des données tout au long du cycle de valeur (Kovrigin & Vasiliev, 2020 ; Prokhin, 2020). La transformation digitale, qui est par nature *un « changement fondamental qui modifie complètement le mode de fonctionnement des organisations dans tous les domaines : développement et conception, production, vente et après-vente »* (Prokhin, 2020 p.131), touche tous les niveaux et toutes les sphères des organisations.

2. Revue de littérature

2.1. La transformation digitale dans les PME : opportunités et défis

En deux décennies, la transformation digitale (TD) a changé de direction. Initialement vouée à l'intégration de systèmes d'information internes (ERP, CRM) pour optimiser les processus et réduire les coûts (Cha, Hwang & Gregor, 2015 ; Besson & Rowe, 2012 ; El Amrani & Saint-Léger, 2013), elle s'est convertie, sous l'effet du big data, de l'IA et de l'IoT, en un vecteur de reconfiguration des modèles d'affaires orientés vers la valeur client et l'internationalisation (Rothberg & Erickson, 2017 ; Cenamor et al., 2019 ; Li et al., 2018 ; Ferraris et al., 2018 ; Rachinger et al., 2018 ; Zott & Amit, 2017 ; Loupiac et al., 2024). Ce passage d'une logique d'efficacité interne à une logique de transformation systémique explique que la TD ne produise ses effets qu'au prix de mutations profondes – stratégie, culture, leadership, compétences – et d'une interdépendance accrue entre fonctions, dont le défaut de coopération constitue un facteur d'échec récurrent (Prokhin, 2020 ; Kovrigin & Vasiliev, 2020).

Pour les petites et moyennes entreprises (PME), ce mouvement représente d'abord une opportunité de rattrapage compétitif : l'analyse de données, la traçabilité par l'IoT et les

plateformes numériques leur permettent de rivaliser avec de plus grandes structures sur la personnalisation de l'offre, l'interaction client et l'accès direct aux marchés internationaux (Li et al., 2018 ; Rachinger et al., 2018 ; Ferraris et al., 2018). L'enjeu décisif n'est toutefois pas l'accès à ces outils, aujourd'hui banalisé, mais leur conversion en avantage durable – ce qui déplace la question de la technologie elle-même vers les capacités organisationnelles requises pour l'exploiter.

Or ces capacités se heurtent, dans les PME, à des contraintes structurelles que la TD ne neutralise pas : ressources financières limitées, déficit de compétences numériques, charge opérationnelle qui pénalise les projets de long terme et exigence de rentabilité rapide des investissements (Goerzig & Bauernhansl, 2018). L'automatisation allège la pression sur les effectifs, mais suppose en retour de nouvelles compétences et configurations homme-machine difficilement mobilisables à court terme ; la dépendance croissante à la qualité des données, à la cybersécurité et à la confidentialité y ajoute des vulnérabilités spécifiques (Kshetri, 2021 ; Kovrigin & Vasiliev, 2020).

Cette tension éclaire la principale limite de la littérature : bien qu'abondante et dynamique (Rêgo et al., 2021 ; Vial, 2019 ; Kraus et al., 2022), elle reste fragmentée, centrée sur les grandes entreprises et focalisée sur des technologies isolées, sans cadre holistique adapté aux PME (Ghosh et al., 2022 ; Kohli & Melville, 2019 ; Ritala et al., 2021). Pour ces dernières, la transition relève moins d'un enjeu technique que d'une capacité d'adaptation organisationnelle et humaine, dimension que la recherche éclaire encore insuffisamment.

2.2. La transformation digitale au service de la gestion de la qualité : le cadre ISO 9001

La transformation digitale (TD) ouvre de larges perspectives pour l'amélioration de la gestion de la qualité (MQ) en réduisant l'impact du facteur humain dans la détection et la prévention des non-conformités et des erreurs (Menshikova et al., 2019 ; Manita et al., 2020). Grâce à divers capteurs, applications et technologies telles que l'Internet des objets (IoT), l'intelligence artificielle (IA), le big data et l'analyse prédictive, les indicateurs de performance peuvent être enregistrés et les processus contrôlés en temps réel (Prokhin, 2020), favorisant ainsi une meilleure traçabilité des produits – particulièrement cruciale dans des secteurs comme l'agroalimentaire et la pharmaceutique – ainsi qu'une intégration plus étroite des exigences clients dans la conception et la fabrication (Matt & Rauch, 2020). La TD permet également d'obtenir des informations centrées sur les données pour concevoir et mettre en œuvre des mesures correctives en temps opportun (Radej et al., 2017), tout en améliorant la révision, l'optimisation et la normalisation des processus et procédures (Mayakova, 2019 ; Menshikova et al., 2019 ; Ivančić et al., 2019). Elle pourrait même devenir l'un des nouveaux principes de gestion de la qualité, au même titre que l'innovation et l'adaptabilité (Mayakova, 2019).

Dans ce contexte, le système de management de la qualité (SMQ) fondé sur la norme ISO 9001 constitue un outil structuré et reconnu internationalement qui permet à l'entreprise de diriger et contrôler les activités liées à l'amélioration continue de la qualité (ISO 9001:2015). Axé sur la

prévention plutôt que sur la correction, il s'appuie sur un cycle d'amélioration continue (Rahman, 2001) et favorise la formalisation des méthodes, l'engagement des employés et la réduction des délais (Heras-Saizarbitoria & Boiral, 2013). Générique et applicable à tout type d'organisation indépendamment de sa taille ou de son secteur, la norme ISO 9001 met l'accent sur l'amélioration des processus plutôt que sur les produits ou services eux-mêmes, tout en exigeant une communication efficace, une autonomisation des employés et une implication transversale de l'ensemble des acteurs pour traiter les questions de qualité et formuler des recommandations d'amélioration (Pereira & Oyadomari, 2014).

Dans les PME, un SMQ garantit le ciblage et le contrôle des activités directement ou indirectement liées à l'obtention des résultats attendus. En général, il comprend la structure organisationnelle, la planification, les processus, les ressources et les informations documentées utilisées pour atteindre les objectifs de qualité (tels que la satisfaction des exigences des clients et des parties prenantes concernées). La certification ISO 9001 apparaît ainsi comme une étape clé vers l'adoption de pratiques avancées de gestion de la qualité (Terziovski & Guerrero, 2014), renforçant la confiance des clients et constituant un socle solide pour intégrer les apports de la transformation digitale dans un cadre structuré et résilient.

La transformation digitale est retenue ici comme une capacité organisationnelle de reconfiguration plutôt que comme une simple adoption d'outils. Cette capacité combine ressources technologiques, compétences humaines, gouvernance des données et alignement stratégique. Appliquée au SMQ, elle agit sur les processus qualité par l'automatisation, la traçabilité, l'intégration des données et la prise de décision fondée sur les preuves. Les travaux empiriques ont été mobilisés comme points d'appui pour identifier les conditions de réussite de la digitalisation du SMQ en PME. Ces travaux convergent vers une idée centrale : l'effet positif des technologies dépend de capacités complémentaires, notamment les compétences, l'alignement stratégique, la culture qualité et la gestion du changement.

Tableau 2 : Enseignements empiriques pour la digitalisation du SMQ en PME

Champ empirique	Travaux mobilisés	Enseignement principal	Implication pour le SMQ numérique
Digitalisation des PME	Li et al. (2018) ; Eller et al. (2020) ; Cenamor et al. (2019)	Les capacités numériques et relationnelles soutiennent l'agilité et l'accès au marché.	La technologie doit être reliée aux processus et aux compétences, pas seulement installée.
Industrie 4.0 et maturité	Moeuf et al. (2018) ; Mittal et al. (2018) ; Matt & Rauch	Les PME adoptent plus facilement des solutions ciblées et progressives.	Prioriser la Gestion Électronique des Documents (GED), la traçabilité et les

Champ empirique	Travaux mobilisés	Enseignement principal	Implication pour le SMQ numérique
	(2020) ; Skrzypek & Lissowski (2025)		indicateurs avant les technologies avancées.
ISO 9001 et pratiques qualité	Rahman (2001) ; Tersiovski & Guerrero (2014) ; Pereira & Oyadomari (2014)	Les bénéfices de la certification dépendent de l'appropriation interne de la mesure.	Le SMQ doit renforcer la preuve, l'auditabilité et l'amélioration continue.
Technologie et qualité	Carvalho et al. (2020) ; Dutta et al. (2021) ; Menshikova et al. (2019) ; Mayakova (2019)	La digitalisation crée de la valeur lorsqu'elle transforme l'approche processus.	L'automatisation doit être accompagnée de gouvernance des données et de cybersécurité.

Source : élaboré par les auteurs

3. Vers le développement d'un système moderne de management de la qualité

3.1. Intégration du SMQ dans le système managérial de l'entreprise

Dans une économie numérique marquée par des mutations rapides et une exigence accrue de réactivité, les PME doivent relever le défi d'une gestion de la qualité à un niveau qualitativement supérieur. La transformation digitale (TD) apparaît comme le levier principal pour restructurer l'environnement interne, optimiser les processus de gestion et intégrer une automatisation profonde du Système de Management de la Qualité (SMQ) (Menshikova et al., 2019). Elle permet de convertir les opérations manuelles – traditionnellement très consommatrices de ressources humaines – en un format numérique, couvrant la collecte et l'analyse de données sur les produits, processus et systèmes, la surveillance continue, la prise de décision fondée sur des preuves, l'adaptation des exigences qualité aux évolutions et l'identification proactive des risques.

Pour les PME, ces évolutions représentent une opportunité stratégique décisive. Les progrès technologiques élargissent considérablement les possibilités de gestion de la qualité en réduisant fortement le « facteur humain » dans les tâches routinières, sans pour autant supprimer totalement l'intervention humaine : la TD élimine la répétition et libère les équipes pour des activités à plus forte valeur ajoutée (Vasiliev & Aleksandrova, 2020 ; Menshikova et al., 2019).

Le véritable enjeu réside dans la refonte des processus et procédures afin que l'humain et les systèmes numériques collaborent efficacement à l'amélioration continue de la qualité.

La norme ISO 9001:2015 accentue cette dynamique en exigeant que le SMQ s'intègre pleinement au système global de gestion de l'entreprise (gestion financière, RH, environnementale, informationnelle), et non plus qu'il reste un sous-système isolé (Sampaio et al., 2009). Cette intégration est particulièrement cruciale pour les PME, dont les ressources limitées rendent d'autant plus nécessaire une approche unifiée et efficace.

Dans une logique de Qualité 4.0, l'approche processus du SMQ repose sur des décisions fondées sur des preuves, alimentées par des données fiables, traçables et actualisées (ISO, 2015 ; Carvalho et al., 2020). Lorsque les données relatives aux processus, aux non-conformités, aux audits et à la satisfaction client sont dispersées ou peu fiables, la capacité de pilotage du SMQ diminue. La transformation digitale permet donc de renforcer la cohérence du système à condition que les données soient gouvernées, sécurisées et intégrées au système global de gestion de l'entreprise (Vasiliev & Aleksandrova, 2020 ; Menshikova et al., 2019).

3.2. La transformation digitale des SMQ et risques numériques

La littérature sur l'interaction entre transformation digitale (TD) et systèmes de management de la qualité (SMQ) reste relativement récente, mais elle converge vers l'idée que la TD exerce un impact profond et multidimensionnel sur ces systèmes (Carvalho et al., 2020 ; Menshikova et al., 2019 ; Mayakova, 2019). Menshikova et al. (2019) soulignent qu'il est désormais nécessaire de transformer les SMQ dans le cadre de l'économie numérique. Ils préconisent une intégration complète du système de gestion de la qualité au sein du système de gestion global de l'organisation, via la mise en place d'une plateforme numérique interne, tout en insistant sur l'impératif d'identifier et de gérer les risques à chaque étape du processus de mise en œuvre. Dans une perspective similaire, Mayakova (2019) démontre que la transformation numérique de la gestion de la qualité produit des effets positifs significatifs sur les organisations. Elle propose un modèle intégré de management de la qualité adapté au contexte d'expansion numérique, fondé sur l'approche processus ; ce modèle, illustré par la figure 1, articule de manière cohérente les domaines clés de la gestion de la qualité et ceux de la transformation numérique.

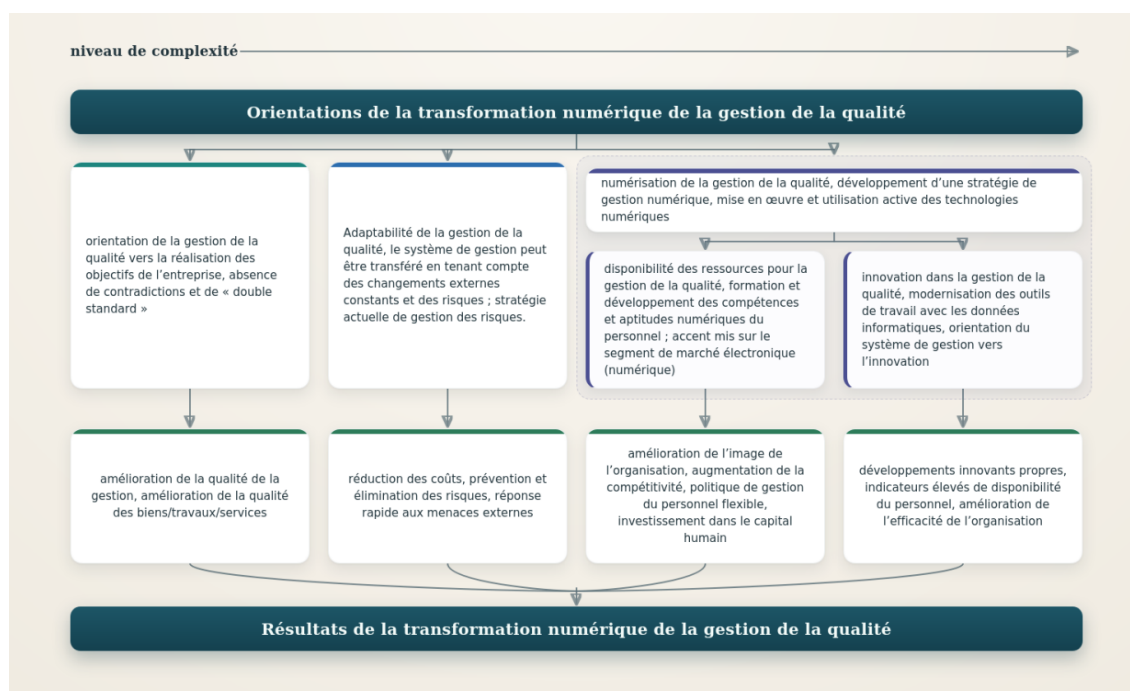


Figure 1 : Modèle de gestion de la qualité dans le contexte de la numérisation totale

Source : Adaptée par les auteurs, Mayakova, 2019

D'autres travaux confirment que la numérisation des SMQ ne se limite pas à une simple modernisation technique : elle modifie également les relations avec les parties prenantes impliquées dans la gestion de la qualité (Manakhova, Levchenko & Esina, 2021) et renouvelle profondément les outils et méthodes mobilisés (Carvalho et al., 2020, Dutta et al., 2021). Ces évolutions entraînent un impact global et systémique sur les SMQ, les rendant plus agiles, et mieux alignés sur les exigences d'une économie numérique.

La transformation digitale du SMQ ne peut être analysée uniquement comme un facteur d'efficacité. Elle augmente aussi la surface d'exposition de l'entreprise et impose une lecture hiérarchisée des risques. Dans les PME, ces risques sont d'autant plus critiques que les ressources de cybersécurité, les compétences internes et la capacité de continuité d'activité sont souvent limitées. La revue permet de distinguer trois niveaux de risques interdépendants : technico-humain, organisationnel et externe (Kshetri, 2021 ; Haque et al., 2025).

Au niveau technico-humain, les cyberattaques, le phishing, les ransomwares, les erreurs de manipulation et les violations de données peuvent affecter directement la maîtrise documentaire, la traçabilité et la preuve de conformité exigées par ISO 9001. Les enjeux de confidentialité et de protection des données, notamment au regard du RGPD, exigent une gouvernance stricte des accès, des sauvegardes et des traitements (Pfleeger & Caputo, 2012 ; Voigt & Von dem Bussche, 2021) ;

Au niveau organisationnel, la résistance au changement, l'insuffisance des compétences numériques et la faible maturité des processus réduisent la robustesse du

SMQ numérique. Une digitalisation partielle, non alignée sur l'approche processus, risque de produire des silos supplémentaires plutôt qu'une meilleure intégration qualité ;



Au niveau externe, la dépendance aux fournisseurs cloud, aux plateformes, aux équipements IoT et aux prestataires de maintenance crée des vulnérabilités de continuité. Une indisponibilité de service, une attaque visant un tiers ou une rupture d'approvisionnement technologique peut bloquer l'accès aux données qualité et fragiliser la maîtrise des processus externalisés.

La TD a non seulement ouvert des perspectives d'innovation et d'efficacité, mais a également augmenté de manière spectaculaire et extrême la surface d'attaque. Ces vulnérabilités, souvent sous-estimées par les PME, peuvent transformer une opportunité digitale en menace existentielle si elles ne sont pas anticipées dès la conception du SMQ numérique. En définitive, la gestion des risques numériques doit être intégrée dès la conception du SMQ numérique. Le tableau 3 suivant synthétise les risques prioritaires, leur criticité et les mesures de maîtrise recommandées pour les PME.

Tableau 3 : Hiérarchisation des risques numériques associés au SMQ numérique

Risque prioritaire	Impact potentiel sur le SMQ	Criticité	Mesures de maîtrise recommandées
Cyberattaques et indisponibilité	Blocage de la GED, perte d'accès aux preuves qualité, rupture de traçabilité.	Élevée	Cybersécurité, sauvegardes, tests de restauration.
Violation de données et confidentialité	Non-conformité réglementaire, perte de confiance client, fragilisation des audits.	Élevée	Chiffrement, droits d'accès, registre des traitements, conformité RGPD (privacy by design).
Mauvaise qualité ou dispersion des données	Décisions erronées, indicateurs qualité peu fiables, actions correctives tardives.	Moyenne à élevée	Référentiels de données, règles de validation, indicateurs de qualité des données.
Dépendance aux fournisseurs cloud / IoT	Interruption de service et perte de maîtrise des processus externalisés.	Moyenne à élevée	Clauses contractuelles, évaluation périodique des prestataires.
Résistance au changement et déficit de compétences	Usage partiel du SMQ numérique, contournement des procédures, perte d'efficacité.	Élevée	Formation, conduite du changement, implication des

Risque prioritaire	Impact potentiel sur le SMQ	Criticité	Mesures de maîtrise recommandées
			utilisateurs, référents qualité-numériques.

Source : élaboré par les auteurs

3.3. Le SMQ numérique et ses technologies : opportunités pour les PME

A l'heure où les technologies de l'information ont toujours soutenu le SMQ (gestion électronique des documents, ERP, CRM), la transformation digitale en modifie la nature même : l'IoT, le big data, la blockchain et l'analyse prédictive ne s'ajoutent plus comme des outils périphériques mais deviennent constitutifs du système (Aleksandrova et al., 2018). Le changement est donc qualitatif plutôt que cumulatif : le basculement des opérations manuelles vers un format numérique fait émerger un environnement où le pilotage de la qualité est nativement digital (Aleksandrova et al., 2018 ; Mandrakov et al., 2020).

Pour les PME, cet ancrage de l'automatisation dans les processus orientés clients (conception, production) constitue un levier d'amélioration continue, en fluidifiant la coordination entre services ; son efficacité demeure toutefois conditionnée par les compétences humaines qui en commandent l'usage (Menshikova et al., 2019).

Concrètement, l'automatisation transfère vers le numérique les tâches qualité les plus consommatrices de ressources humaines – collecte et analyse des données, surveillance et mesure, décision fondée sur les preuves, identification des risques. Menshikova et al. (2019) en dégagent quatre priorités convergentes : la gestion électronique de la documentation, l'automatisation de la surveillance et des audits, le contrôle statistique de la qualité et le suivi de la satisfaction client.

Ces SMQ numériques, conçus pour des organisations agiles et centrées sur le client, visent à réduire les coûts et à accélérer l'accès à une information fiable et opportune, améliorant ainsi la décision et la communication interne comme externe (Busch et al., 2018). Dans cette logique, Menshikova et al. (2019) identifient quatre étapes clés de la numérisation du SMQ (figure 2) : *enregistrement et analyse des données ; preuve de conformité aux exigences (documents réglementaires, spécifications) ; surveillance et contrôle des processus du SMQ ; et prise de décision dans des situations ambiguës.*

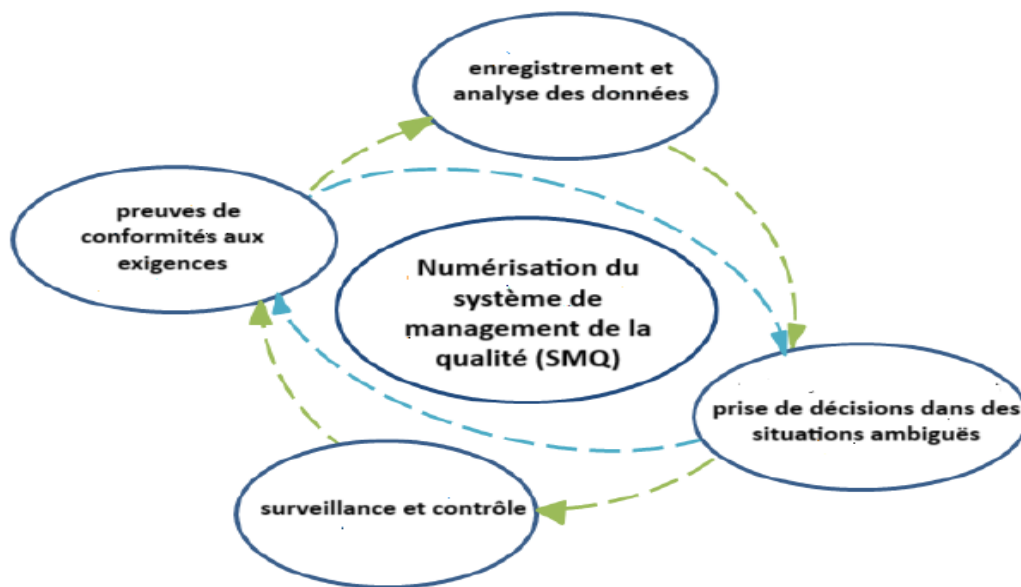


Figure 2 : Les principales étapes de la numérisation du SMQ

Source : Adaptée par les auteurs, Menshikova et al., (2019)

Pour les PME, la mise en place d'un tel SMQ numérique moderne recentre l'effort sur l'amélioration continue des processus internes et génère des effets économiques tangibles, à condition de disposer d'une base de données fiable pour des décisions fondées sur les preuves (Aleksandrova et al., 2018). Le fonctionnement d'un système de gestion de la qualité moderne devient une condition essentielle pour atteindre un niveau de performance élevé et stabiliser les indicateurs de qualité des produits et services. L'apport décisif de la TD tient ici à ce qu'elle renforce l'approche processus – principe central du SMQ moderne, qui agit sur les processus plutôt que sur leurs seuls résultats – avec un rapport coût-efficacité particulièrement favorable à leur intégration dans les PME.

3.4. Modèle conceptuel intégrateur

Le modèle conceptuel proposé ci-dessous (figure 3) synthétise les résultats de la revue et répond à la nécessité de formaliser un cadre d'analyse intégrée.

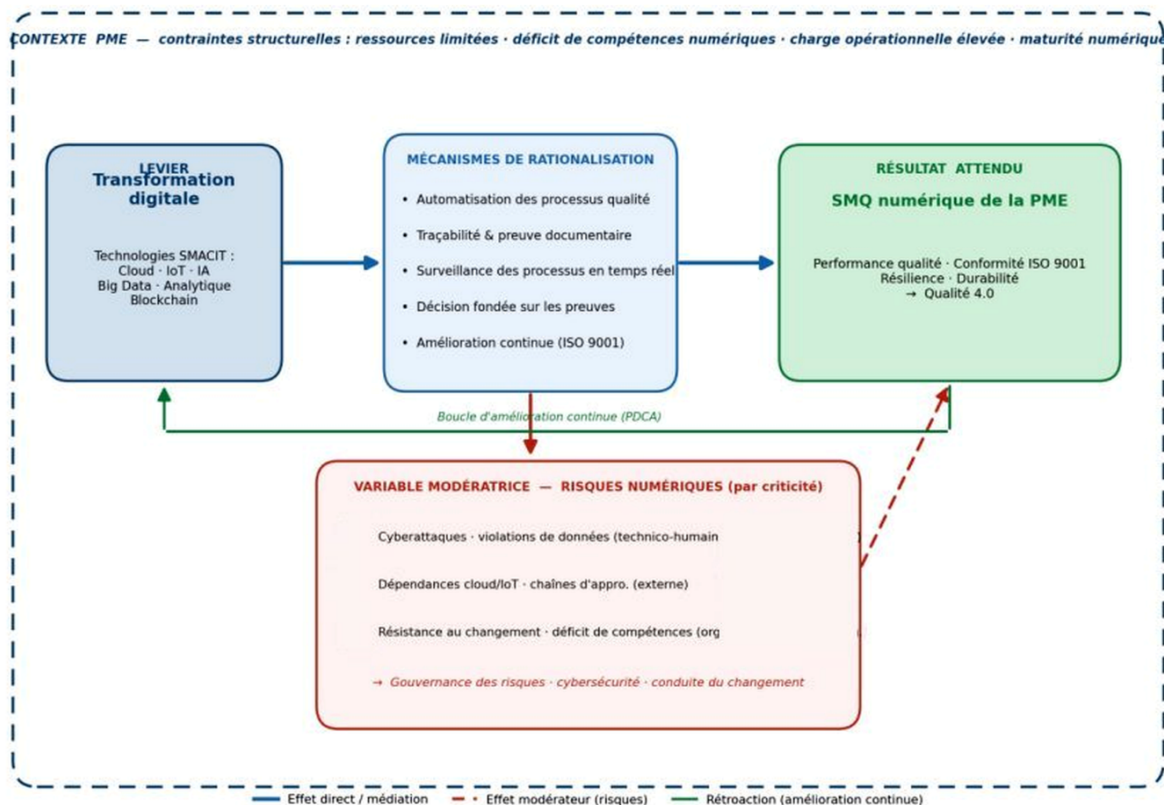


Figure 3 : Modèle conceptuel intégrateur de la digitalisation du SMQ dans les PME

Source : élaboré par les auteurs

Le modèle conceptuel intégrateur (figure 3) synthétise les apports de la revue de littérature en quatre dimensions analytiques articulées. La transformation digitale, mobilisant les technologies SMACIT, constitue le levier (variable explicative). Elle agit sur le SMQ via quatre mécanismes de rationalisation (variables médiatrices) : automatisation des processus qualité, traçabilité et preuve documentaire, surveillance en temps réel et décision fondée sur les preuves. Les risques numériques, hiérarchisés par criticité (tableau 2), jouent un rôle modérateur susceptible d'atténuer, voire d'inverser, les bénéfices attendus. La variable dépendante — un SMQ numérique performant, conforme à l'ISO 9001, résilient et durable (perspective Qualité 4.0) — est elle-même réinjectée dans le levier par une boucle d'amélioration continue (logique PDCA). L'ensemble est encadré dans le contexte spécifique des PME, dont les contraintes structurelles conditionnent l'intensité de chaque relation. Ce modèle constitue une grille d'analyse mobilisable pour de futures validations empiriques.

Tableau 4 : Dimensions analytiques du cadre conceptuel

Dimension	Définition retenue	Indicateurs / variables mobilisables
Maturité numérique	Capacité de la PME à mobiliser des outils numériques de manière cohérente avec ses processus.	ERP / CRM, cloud, GED, compétences numériques, qualité des données.
Digitalisation du SMQ	Intégration des technologies numériques aux activités de planification, contrôle, audit et amélioration.	Maîtrise documentaire, traçabilité, surveillance, audits, CAPA, satisfaction client.
Gouvernance des risques numériques	Ensemble des règles permettant de sécuriser les données, les accès et la continuité du SMQ.	Sauvegardes, droits d'accès, cartographie des risques, plan de continuité.
Performance du SMQ	Effets attendus de la digitalisation sur la maîtrise qualité et la résilience.	Réduction des non-conformités, rapidité de décision, conformité ISO, satisfaction client.

Source : élaboré par les auteurs à partir de Vial (2019), Verhoef et al. (2021), Carvalho et al. (2020) et Kshetri (2021).

Conclusion :

Cette étude démontre que la transformation digitale représente un levier structurant pour rationaliser la mise en œuvre du SMQ dans les PME, mais seulement lorsqu'elle est articulée à l'approche processus, à la gouvernance des données et à la maîtrise des risques numériques. Les résultats de la revue suggèrent que la digitalisation du SMQ ne produit pas mécaniquement de performance. Son efficacité dépend de la cohérence entre technologies, processus et capacités humaines.

Sur le plan théorique, le chapitre contribue à la littérature sur la Qualité 4.0 en montrant que le SMQ numérique ne se réduit pas à l'automatisation des procédures. Il correspond à un système sociotechnique dans lequel les technologies numériques, les compétences humaines, les routines qualité et la cybersécurité interagissent. Cette lecture intégrée permet de dépasser les approches additivement centrées sur les outils et de poser les bases d'un cadre d'analyse testable empiriquement. Ainsi, ce chapitre apporte trois contributions explicites. Premièrement, il propose un modèle conceptuel intégrateur (figure 3) qui articule, dans un même cadre, le levier digital, les mécanismes de rationalisation du SMQ, les risques numériques modérateurs et la performance qualité, là où la littérature antérieure traitait ces éléments séparément. Deuxièmement, il opérationnalise les dimensions de l'analyse en variables mobilisables (explicative, médiatrices, modératrice, dépendante), ouvrant la voie à des tests empiriques. Troisièmement, il introduit une taxonomie des risques numériques par criticité (tableau 2),

enrichissant la lecture habituellement indifférenciée des risques dans les travaux sur la Qualité 4.0.

Sur le plan managérial, les dirigeants de PME sont invités à adopter une trajectoire progressive : diagnostiquer la maturité numérique, prioriser les processus qualité à digitaliser, sécuriser les données critiques, former les acteurs et évaluer régulièrement les risques résiduels. La digitalisation du SMQ doit ainsi être pensée comme un portefeuille de projets alignés sur les ressources réelles de l'entreprise et non comme un basculement technologique uniforme. Cette discussion renforce l'idée que la Qualité 4.0 doit être comprise comme une transformation organisationnelle et non comme une simple modernisation technique.

Les limites de cette recherche tiennent principalement à sa nature conceptuelle et à l'absence de validation empirique directe. La revue systématisée et intégrative permet d'organiser les connaissances existantes, mais elle ne mesure pas encore l'intensité des relations proposées entre maturité numérique, digitalisation du SMQ, gouvernance des risques et performance qualité. Sur le plan méthodologique, l'étude repose sur une revue de littérature : le modèle proposé demeure conceptuel et n'a pas encore fait l'objet d'une validation empirique. Sur le plan du périmètre, la catégorie « PME » est traitée de manière globale, alors que la taille, le secteur, le niveau de réglementation et le degré de dépendance technologique modulent fortement les relations modélisées. Sur le plan documentaire enfin, la prédominance de sources anglophones et l'hétérogénéité des contextes étudiés limitent la transférabilité directe des conclusions.

Les recherches futures pourraient opérationnaliser le modèle proposé à travers des études de cas multiples, des enquêtes quantitatives auprès de PME certifiées ISO 9001 et des approches longitudinales suivant les trajectoires de digitalisation du SMQ. Trois pistes sont prioritaires : mesurer l'effet de la maturité numérique sur la performance du SMQ, tester le rôle modérateur de la gouvernance des risques numériques et comparer les trajectoires sectorielles de digitalisation qualité. Ces travaux permettraient de transformer le modèle conceptuel en instrument empirique d'évaluation et d'aide à la décision.

En définitive, la convergence entre transformation digitale et gestion de la qualité n'est ni une simple tendance passagère, ni une solution miracle. Elle représente un nouveau paradigme, complexe mais structurant, qui oblige les PME à repenser leur rapport à la qualité dans un environnement numérique instable ; celles capables de conjuguer prudence, agilité et vision stratégique seront les mieux armées pour renforcer leur compétitivité et leur pérennité.

Références bibliographiques :

Aleksandrova, S. V., Vasiliev, V. A., Letuchev, G. M. (2018). Digital Technology and Quality Management. *2018 IEEE International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*.
[DOI:10.1109/ITMQIS.2018.8525075](https://doi.org/10.1109/ITMQIS.2018.8525075)

- Besson, M., Gossart, C., & Jullien N. (2017). Les enjeux de la transformation numérique dans l'entreprise du futur. *Terminal, Technologie de l'information culture & société*, n° 120. [DOI:10.4000/terminal.1607](https://doi.org/10.4000/terminal.1607)
- Besson, P., & Rowe, F. (2012). Strategizing information systems-enabled organizational transformation: A transdisciplinary review and new directions. *The Journal of Strategic Information Systems*, 21(2), 103-124. [DOI: 10.1016/j.jsis.2012.05.001](https://doi.org/10.1016/j.jsis.2012.05.001)
- Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital Business Strategy: Toward A Next Generation of Insights. *MIS Quarterly*, 37(2), 471-482. <https://doi.org/10.25300/MISQ/2013/37:2.3>
- Busch, P. A., Henriksen, H. Z., & Sæbø, O. (2018). Opportunities and challenges of digitized discretionary practices: a public service worker perspective. *Government Information Quarterly*, 35 (4), 547-556. <https://doi.org/10.1016/j.giq.2018.09.003>
- Carvalho, A. M. D., Sampaio, P., Rebentisch, E., & Oehmen, J. (2020). Technology and quality management: A review of concepts and opportunities in the digital transformation. *International Conference on Quality Engineering and Management*, 698-714.
- Cenamor, J., Parida, V., & Wincent, J. (2019). How entrepreneurial SMEs compete through digital platforms: The roles of digital platform capability, network capability and ambidexterity. *Journal of Business Research*, 100, 196-206. <https://doi.org/10.1016/j.jbusres.2019.03.035>
- Cha, K. J., Hwang, T., & Gregor, S. (2015). An integrative model of IT-enabled organizational transformation: A multiple case study. *Management Decision*, 53(8), 1755-1770. <https://doi.org/10.1108/MD-09-2014-0550>
- El Amrani R., & Léger G. S. (2013). États des lieux de la recherche ERP francophone. *Systèmes d'information & management*, 18(2), 111-160. [DOI:10.3917/sim.132.0111](https://doi.org/10.3917/sim.132.0111)
- Dutta, G., Kumar, R., Sindhwani, R., & Singh, R. K. (2021). Digitalization priorities of quality control processes for SMEs: a conceptual study in perspective of Industry 4.0 adoption. *Journal of intelligent manufacturing*, 32(6), 1679-1698. [DOI: 10.1007/s10845-021-01783-2](https://doi.org/10.1007/s10845-021-01783-2)
- Eller, R., Alford, P., Kallmünzer, A., & Peters, M. (2020). Antecedents, consequences, and challenges of small and medium-sized enterprise digitalization. *Journal of Business Research*, 112, 119-127. <https://doi.org/10.1016/j.jbusres.2020.03.004>
- Ferraris, A., Monge, F., & Mueller, J. (2018). Ambidextrous IT capabilities and business process performance: an empirical analysis. *Business Process Management Journal*, 24(5), 1077-1090. <https://doi.org/10.1108/BPMJ-07-2017-0201>
- Fitzgerald, M., Kruschwitz, N., Bonnet, D., & Walch, M. (2013). Embracing Digital Technology: A New Strategic Imperative. *MIT Sloan Management Review*. <https://doi.org/10.1016/j.procir.2017.12.257>
- Ghosh, S., Mandal, M.C., & Ray, A. (2022). Exploring the influence of critical parameters on green supply chain management performance of small and medium-sized enterprise: An integrated multivariate analysis-robust design approach. *Cleaner Logistics and Supply Chain*, 4. <https://doi.org/10.1016/j.clscn.2022.100057>
- Goerzig, D., & Bauernhansl, T. (2018). Enterprise Architectures for the Digital Transformation in Small and Medium-Sized Enterprises. *Procedia CIRP*, 67, 540-545. <https://doi.org/10.1016/j.procir.2017.12.257>

- Haque, G. M. M., Akula, D. K., Mohammed, Y. S., Sayed, A., Arafat, Y. (2025). Cybersecurity risk management in the age of digital transformation: A Systematic literature review. *The American Journal of Engineering and Technology*, 7(8), 126-150. <https://doi.org/10.37547/tajet/Volume07Issue08-14>
- Heras-Saizarbitoria I., & Boiral O. (2013). ISO 9001 and ISO 14001: Towards a Research Agenda on Management System Standards. *International Journal of Management Reviews*, 15(1), 47-65. [DOI:10.1111/j.1468-2370.2012.00334.x](https://doi.org/10.1111/j.1468-2370.2012.00334.x)
- Hess, T., Matt, C., Benlian, A. & Wiesböck, F. (2020). *Options for Formulating a Digital Transformation Strategy*. Strategic Information Management.
- Hinings, B., Gegenhuber, T., & Greenwood, R. (2018). Digital innovation and transformation: An institutional perspective. *Information and Organization*. 28(1), 52–61. <https://doi.org/10.1016/j.infoandorg.2018.02.004>
- Ivančić, L., Vukšić, V. Bj., & Spremić, M. (2019). Mastering the Digital Transformation Process: Business Practices and Lessons Learned. *Technology Innovation Management Review*, 9(2), 36-50. [DOI:10.22215/timreview/1217](https://doi.org/10.22215/timreview/1217)
- ISO (2015). Standard ISO 9001:2015 – Quality management systems – requirements. ISO Central Secretariat, Geneva.
- Kshetri, N. (2021). *Cybersecurity management: An organizational and strategic approach*. University of Toronto Press.
- Kohli, R., & Melville, N. P. (2019). Digital innovation: A review and synthesis. *Information Systems Journal*, 29(1), 200–223. [DOI:10.1111/isj.12193](https://doi.org/10.1111/isj.12193)
- Kovrigin, E.A., & Vasiliev, V.A. (2020). Approaches and Problems to Assessing Readiness for the Implementation of Modern Digital Technologies in a Quality Management System. *2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, 336-340. [DOI:10.1109/ITQMIS51053.2020.9322916](https://doi.org/10.1109/ITQMIS51053.2020.9322916)
- Kraus, S., Durst, S., Ferreira, J. J., Veiga, P., Kailer, N., & Weinmann, A. (2022). Digital transformation in business and management research: An overview of the current status quo. *International Journal of Information Management*, 63. <https://doi.org/10.1016/j.ijinfomgt.2021.102466>
- Liu, D. Y., Chen, S. W., & Chou, T. C. (2011). Resource fit in digital transformation – Lessons learned from the CBC bank global e-banking project. *Management Decision*, 49(10), 1728–1742. <https://doi.org/10.1108/00251741111183852>
- Li, L., Su, F., Zhang, W., & Mao, J. Y. (2018). Digital transformation by SME entrepreneurs: A capability perspective. *Information Systems Journal*, 28(6), 1129–1157. <https://doi.org/10.1111/isj.12153>
- Loupiac, P., Le Naggard, E., & Herbinet, V. (2024). La réalité augmentée peut-elle remplacer l’essai physique pour l’achat de biens d’expérience en ligne ? *Décisions Marketing*, 1(113), 95-118. <https://doi.org/10.3917/dm.113.0095>
- Manakhova, I. V., Levchenko, E. V., & Esina, A. R. (2021). Models of Transforming Quality Management Systems in the Digital Company. *Vestnik of Plekhanov Russian University of Economics*, 18(1), 115-123. <https://doi.org/10.21686/2413-2829-2021-1-115-123>

- Mandrakov E. S., Vasiliev A., Dudina D. A. (2020). Non-conforming Production Management in a Digital Quality Management System. *2020 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*. DOI:10.1109/ITQMIS51053.2020.9322931
- Manita, R., Elommal, N., Baudier, P., & Hikkerova, L. (2020). The digital transformation of external audit and its impact on corporate governance. *Technological Forecasting and Social Change*, 150. <https://doi.org/10.1016/j.techfore.2019.119751>
- Matt, C., Hess, T., & Benlian, A. (2015). Digital Transformation Strategies. *Business & Information Systems Engineering*. 57(2), 339-343. DOI:10.1007/s12599-015-0401-5
- Matt, D.T., & Rauch, E. (2020). SME 4.0: The Role of Small- and Medium-Sized Enterprises in the Digital Transformation. In: Matt, D.T., Modrák, V. and Zsifkovits, H., Eds., *Industry 4.0 for SMEs: Challenges, Opportunities and Requirements*, Springer, Berlin, 3-36. https://doi.org/10.1007/978-3-030-25425-4_1
- Mayakova, A. (2019). Digital transformation of modern quality management. *Economic Annals-XXI*, 180(11-12), 138-145. DOI: <https://doi.org/10.21003/ea.V180-15>
- Menshikova, M. A., Piunova Y. V., & Makhova M. N. (2019). Digital Transformation in the Quality Management System. DOI:10.1109/ITQMIS.2019.8928438
- Mittal, S., Khan, M. A., Romero, D., & Wuest, T. (2018). A critical review of smart manufacturing & Industry 4.0 maturity models: Implications for small and medium-sized enterprises. *Journal of Manufacturing Systems*, 49, 194-214. <https://doi.org/10.1016/j.jmsy.2018.10.005>
- Moeuf, A., Pellerin, R., Lamouri, S., Tamayo-Giraldo, S., & Barbaray, R. (2018). The industrial management of SMEs in the era of Industry 4.0. *International Journal of Production Research*, 56(3), 1118-1136. <https://doi.org/10.1080/00207543.2017.1372647>
- Parviainen, P., Tihinen, M., Käräriäinen, J., & Teppola S. (2017). Tackling the digitalization challenge: How to benefit from digitalization in practice. *International Journal of Information Systems and Project Management*, 5(1), 63–77. DOI: 10.12821/ijispm050104
- Pereira, D. S., & Oyadomari J. C. T. (2014). Performance Measurement System and Quality Management in Small and Medium-Sized Brazilian Enterprises. *Research in Accounting in Emerging Economies*, 14, 151-184. DOI:10.1108/S1479-356320140000014005
- Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cybersecurity risk. *Computers & Security*, 31, 597-611. DOI:10.1016/j.cose.2011.12.010
- Prokhin, E. (2020). Digital Transformation of Industrial Companies: What is Management 4.0? *Proceedings of the 2020 11th International Conference on E-business, Management and Economics*, 131-138. <https://doi.org/10.1145/3414752.3414779>
- Rachinger, M., Rauter, R., Müller, C., Vorraber, W., & Schirgi E. (2018). Digitalization and its influence on business model innovation. *Journal of Manufacturing Technology Management*, 30(8), 143-1160. <https://doi.org/10.1108/JMTM-01-2018-0020>
- Radej, B. A., Drnovšek, J. A., & Begeš, G. (2017). An overview and evaluation of quality improvement methods from the manufacturing and supply-chain perspective. *Advances in Production Engineering & Management*, 12(4), 388-400.

<https://doi.org/10.14743/apem2017.4.266>

Rahman, S. (2001). A Comparative Study of TQM Practice and Organizational Performance of SMEs with and without ISO Certification. *International Journal of Quality and Reliability Management*, 18(1), 35-49.

<https://doi.org/10.1108/02656710110364486>

Rêgo, B.S., Jayantilal, S., Ferreira, J.J., & Carayannis, E.G. (2021). Digital Transformation and Strategic Management: a Systematic Review of the Literature. *Journal of the knowledge economy*, 13, 3195–3222. DOI: [10.1007/s13132-021-00853-3](https://doi.org/10.1007/s13132-021-00853-3)

Rothberg, H. N., & Erickson, G. S. (2017). Big data systems: knowledge transfer or intelligence insights? *Journal of Knowledge Management*, 21(1), 92-112.

DOI:[10.1108/JKM-07-2015-0300](https://doi.org/10.1108/JKM-07-2015-0300)

Ritala, P., Baiyere, A., Hughes, M., & Kraus, S. (2021). Digital strategy implementation: The role of individual entrepreneurial orientation and relational capital, *Technological Forecasting and Social Change*. 171. <https://doi.org/10.1016/j.techfore.2021.120961>

Sampaio, P., Saraiva, P., & Rodrigues, A. G. (2009). ISO 9001 certification research: Questions, answers and approaches. *International Journal of Quality & Reliability Management*, 26(1), 38–58. <https://doi.org/10.1108/02656710910924161>

Schallmo, D., Williams, C. A., & Boardman, L. (2019). Digital Transformation of Business Models—Best Practice, Enablers, And Roadmap. In *Digital Disruptive Innovation* 36, 119–138. https://doi.org/10.1142/9781786347602_0005

Skrzypek E., & Lissowski, O. (2025). Quality 4.0 in the Context of Industry 4.0: Theoretical Aspects and Research Results, *European Research Studies Journal*, 28(2), 529-540. DOI: [10.35808/ersj/3994](https://doi.org/10.35808/ersj/3994)

Snyder, H. (2019). Literature Review as a Research Methodology: An Overview and Guidelines. *Journal of Business Research*, 104, 333-339. <https://doi.org/10.1016/j.jbusres.2019.07.039>

Terziovski, M., & Guerrero, J. L. (2014). ISO 9000 quality system certification and its impact on product and process innovation performance. *International Journal of Production Economics*, 158, 197-207. DOI:[10.1016/j.ijpe.2014.08.011](https://doi.org/10.1016/j.ijpe.2014.08.011)

Torraco, R.J. (2005). Writing Integrative Literature Reviews: Guidelines and Examples. *Human Resource Development Review*, 4(3), 356-367.

<https://doi.org/10.1177/1534484305278283>

Varenne, P., Godé, C. (2023). *La Transformation Digitales du Modèle d’Affaire : vers un Business Model Digital Dynamique (BMD²) à destinations des PME*. Editions EMS, Caen.

Vasiliev, V. A., & Aleksandrova, V. S. (2020). The Prospects for the Creation of a Digital Quality Management System DQMS. *2020 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*. DOI:[10.1109/ITQMIS51053.2020.9322890](https://doi.org/10.1109/ITQMIS51053.2020.9322890)

Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J.Q., Fabian, N., & Haenlein M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*, 122, 889-901.

<https://doi.org/10.1016/j.jbusres.2019.09.022>

- Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *Journal of Strategic Information Systems*, 28 (2), 118–144.
<https://doi.org/10.1016/j.jsis.2019.01.003>
- Voigt, P., & Von dem Bussche, A. (2021). *The EU General Data Protection Regulation (GDPR)*. Springer.
- Wang, L., & Yan, J. (2023). Effect of digital transformation on innovation performance in China: corporate social responsibility as a moderator. *Frontiers in Environmental Science*, 11.
<https://doi.org/10.3389/fenvs.2023.1215866>
- Warner, K. S.R., & Wäger, M. (2019). Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal. *Long Range Planning*, 52(3), 326-349.
<https://doi.org/10.1016/j.lrp.2018.12.001>
- Westerman, G., Bonnet, D., & McAfee, A. (2014). The Nine Elements of Digital Transformation. *MIT Sloan Management Review*, 55, 1-6.
- Wiersh, E.M., & Autissier, D. (2016). *La Transformation Digitales des Entreprises : les bonnes pratiques*. Editions Eyrolles, Paris.
- Zott, C., & Amit, R. (2017). Business Model Innovation: How to Create Value in a Digital World. *NIM Marketing Intelligence Review*, 9(1), 18-23.
<https://doi.org/10.1515/gfkmir-2017-0003>

Management du risque et conduite du changement

Cet ouvrage collectif est le fruit des travaux de la première édition de la Journée Scientifique « Management du Risque et Conduite du Changement » (MRCC), organisée par l'équipe de recherche en Entrepreneuriat, Marketing, Audit et gouvernance - EMAG ; relevant de l'École Nationale de Commerce et de Gestion d'Oujda (ENCG Oujda). Il s'inscrit dans une double perspective, à la fois scientifique et managériale.

Sur le plan scientifique, il contribue à l'enrichissement de la littérature consacrée au management du risque et à la conduite du changement, en mobilisant une diversité d'approches théoriques, conceptuelles et méthodologiques.

Sur le plan managérial et professionnel, il met à la disposition des décideurs, managers, auditeurs et autres parties prenantes des analyses, outils et pistes d'action susceptibles de favoriser l'anticipation des risques, l'adaptation organisationnelle et le renforcement de la résilience des organisations.

La diversité des contributions repose également sur la mobilisation de plusieurs disciplines et champs de recherche, notamment le management, la finance, l'audit, le contrôle, les systèmes d'information, le droit, la logistique, l'économie et les sciences sociales. Cette approche pluridisciplinaire permet de croiser les perspectives et de mieux appréhender la complexité des phénomènes étudiés.

Ainsi, cet ouvrage se veut à la fois un support de réflexion scientifique, un espace de dialogue entre différentes disciplines et un outil d'aide à la décision, contribuant à une meilleure compréhension des interactions entre management du risque, gouvernance, transformation organisationnelle et conduite du changement dans un environnement marqué par l'incertitude, la complexité et l'accélération des mutations.

Sous la direction :

Nisrine OURIACHI · Nour El Houda MOKHTARI · Majda ALAOUI

