International journal of applied management and economics
Vol : 02 , N° 13, Avril 2025
ISSN : 2509-0720

L'impact de la transformation digitale sur le dispositif de contrôle interne des entreprises marocaines

The impact of digital transformation on the internal control system of Enterprises.

- **Auteur 1 :** ACHTOUK Amina,
- **Auteur 2 :** BOUAZIZ Si Mohamed,

(1) Docteure, Laboratoire de Recherche en Entreprenariat, Finance et Management des Organisations (LAREFMO), FSJES Agadir, Université IBN ZOHR.

(2) Enseignant-Chercheur, Laboratoire de Recherche en Entreprenariat, Finance et Management des Organisations (LAREFMO), FSJES Agadir, Université IBN ZOHR.

Conflit d'intérêt : L'auteur ne signale aucun conflit d'intérêt.

Pour citer cet article : ACHTOUK .A & BOUAZIZ .Si M (2025) « L'impact de la transformation digitale sur le dispositif de contrôle interne des entreprises marocaines»,

IJAME : Volume 02, N° 13 | Pp: 361 – 377.

Date de soumission : Mars 2025
Date de publication : Avril 2025

DOI : 10.5281/zenodo.15304014
Copyright © 2025 – IJAME

Résumé

Dans un contexte marqué par une évolution technologique rapide, la transformation digitale s'impose comme un levier stratégique majeur pour les organisations. Cette mutation, qui touche aussi bien les processus opérationnels que les systèmes d'information, redéfinit en profondeur les mécanismes de gouvernance et de gestion des risques. Le contrôle interne, pilier essentiel de la performance et de la conformité des entreprises, n'échappe pas à cette dynamique. À travers le prisme du référentiel COSO, structuré autour de cinq volets fondamentaux - l'environnement de contrôle, l'évaluation des risques, les activités de contrôle, l'information et la communication, ainsi que le pilotage - cet article analyse l'impact de la transformation digitale sur la qualité et l'efficacité du contrôle interne. Il a été démontré que la transformation numérique a un impact positif sur l'amélioration de la qualité du contrôle interne des entreprises.

Mots clés : Transformation digitale, contrôle interne, gestion des risques, COSO, environnement de contrôle

Abstract

In a context marked by rapid technological evolution, digital transformation is emerging as a major strategic lever for organizations. This change, which affects both operational processes and information systems, is profoundly redefining governance and risk management mechanisms. Internal control, a key pillar of corporate performance and compliance, is no exception to this dynamic. Through the prism of the COSO framework, structured around five fundamental components - control environment, risk assessment, control activities, information and communication, and Monitoring Activities - this article analyzes the impact of digital transformation on the quality and effectiveness of internal control. It has been demonstrated in detail that digital transformation has a positive impact on improving the quality of companies' internal control.

Keywords : Digital transformation, internal control, risk management, COSO, control environment

Introduction

Dans un environnement économique de plus en plus complexe et interconnecté, la transformation digitale s'impose comme un phénomène incontournable, porteur de profondes mutations pour les organisations publiques et privées. Ac
célérée par les avancées technologiques récentes, telles que l'intelligence artificielle, le big data, le cloud computing ou encore la robotisation des processus, cette dynamique de digitalisation redéfinit les logiques organisationnelles, les modes de création de valeur et les pratiques de gouvernance. Elle ne se limite pas à l'intégration d'outils technologiques, mais implique une reconfiguration globale des processus métiers, des modèles de pilotage et des systèmes d'information.

Dans ce contexte, la fonction de contrôle interne, historiquement centrée sur la prévention des risques, l'assurance de la conformité et la fiabilité de l'information financière, se trouve au cœur de cette transformation. Les enjeux liés à la digitalisation obligent les entreprises à repenser en profondeur leur dispositif de contrôle interne afin de garantir son efficacité, sa résilience et son agilité face aux nouveaux risques émergents, notamment cybernétiques et opérationnels. Dès lors, une question centrale se pose : **comment la transformation digitale influence-t-elle la qualité et la performance du dispositif de contrôle interne des entreprises ?**

Cette réflexion s'inscrit dans une double approche théorique. D'une part, la théorie de la contingence met en évidence l'importance de l'ajustement des systèmes de contrôle interne en fonction des caractéristiques de l'environnement externe : dans un contexte fortement digitalisé, le contrôle interne doit nécessairement s'adapter pour rester pertinent et efficace. D'autre part, la théorie de l'automatisation cognitive explique comment les technologies d'intelligence artificielle peuvent transformer en profondeur les mécanismes de contrôle et de conformité, en permettant une automatisation intelligente, une détection proactive des anomalies, et une prise de décision plus rapide et fondée sur les données.

À partir de ces fondements théoriques, cet article propose d'analyser l'impact de la transformation digitale sur la qualité du contrôle interne, à la lumière du référentiel COSO, structuré autour de cinq composantes clés : l'environnement de contrôle, l'évaluation des risques, les activités de contrôle, l'information et la communication, et le pilotage. L'objectif est de démontrer que la digitalisation, loin de fragiliser le contrôle interne, peut au contraire en renforcer la robustesse, la réactivité et l'efficience.

Pour ce faire, cet article s'articule en trois parties. La première est consacrée à une revue de littérature, définissant la transformation digitale et le contrôle interne, en s'appuyant sur les

objectifs et les composantes du dispositif selon le référentiel COSO. La deuxième partie expose le cadre théorique de la recherche, fondé sur les théories de la contingence et de l'automatisation cognitive. Enfin, la troisième partie présente l'impact concret de la transformation digitale sur le dispositif de contrôle interne des organisations.

1. Revue de littérature

Avant d'analyser les effets de la transformation digitale sur le contrôle interne, il est essentiel de clarifier les concepts clés mobilisés dans cette étude. Cette première partie propose ainsi une revue de littérature qui vise, d'une part, à définir la transformation digitale et à en cerner les enjeux organisationnels, et d'autre part, à présenter le dispositif de contrôle interne à travers ses objectifs et ses composantes fondamentales, telles que définies par le référentiel COSO. Cette mise en perspective théorique permet de poser les bases nécessaires à une compréhension approfondie des interactions entre digitalisation et contrôle interne.

1.1. La transformation digitale

La transformation digitale peut être définie comme un processus stratégique et organisationnel par lequel une entreprise intègre de manière progressive et cohérente les technologies numériques dans l'ensemble de ses activités, afin d'améliorer sa performance, son agilité et sa capacité d'innovation. Elle ne se limite pas à la simple numérisation des processus existants, mais implique une reconfiguration profonde des modèles opérationnels, de la culture organisationnelle et des modes de création de valeur (Bloching et al., 2015).

Selon Westerman, et al., (2014), elle représente un levier puissant permettant aux entreprises de repenser leurs opérations, leurs produits et leurs services afin de rester compétitives dans un environnement en constante évolution. Ce processus implique non seulement l'intégration de solutions technologiques innovantes, mais aussi une transformation culturelle et organisationnelle, nécessaire pour exploiter pleinement le potentiel du numérique.

Tableau 1 : Définitions de la transformation digitale

Auteurs	Définitions
Fitzgerald et al. 2013	« La définition de la transformation digitale est basée sur l'utilisation de nouvelles technologies digitales telles que la technologie mobile, les réseaux sociaux, les outils analytiques ou intégrés ».
Bowersox et al. 2005	« La transformation digitale est le processus de changement au sein d'une entreprise afin d'intégrer le numérique dans ses opérations et développer des relations larges dans la chaîne d'approvisionnement ».
Solis et al. 2014	« La mise en place de nouveaux investissements et la restructuration dans le cadre de l'intégration de la technologie et des modèles d'affaire pour appréhender plus efficacement les clients numériques au niveau de chaque point de contact du cycle de vie de l'expérience client ».
Hanelt et al. 2020	« La transformation digitale est définie comme le changement organisationnel provoqué et façonné par une expansion généralisée de la technologie numérique. Ce changement implique une transition vers des modèles organisationnels flexibles et malléables qui sont incorporés dans des écosystèmes d'activités numériques ».
Verhoef et al. 2021	« La transformation est déterminée par un changement dans la façon dont une entreprise met en œuvre les technologies numériques, dans le but de développer un nouveau modèle commercial numérique qui permet d'évoluer et créer plus de valeur pour l'entreprise ».
Mazzone, DM 2014	« La transformation digitale est l'évolution numérique volontaire et continue d'une entreprise et cela à travers l'évolution de son modèle d'entreprise, de son processus d'idée ou méthodologie, et d'une transition à la fois stratégiquement et tactiquement ».
Martin 2008	« La transformation digitale est maintenant communément interprétée comme un tel usage des technologies de l'information et de la communication, lorsque l'on n'effectue pas une automatisation triviale, mais que de nouvelles capacités sont créées dans les entreprises, les administrations publiques, ainsi que dans la vie des personnes et de la société ».

Source : Loulid et Hefnawi, (2021)

1.2. Le contrôle interne selon le référentiel COSO

Le COSO (Committee of Sponsoring Organizations of the Treadway Commission) a été fondé en 1985 dans le but de renforcer la fiabilité de l'information financière et de promouvoir des pratiques de gouvernance éthique et efficace au sein des organisations. En 1992, cet organisme publie le cadre de référence intitulé « Internal Control - Integrated Framework », communément appelé COSO 1. Ce

modèle constitue une approche structurée visant à aider les entreprises à concevoir, mettre en œuvre, évaluer et améliorer leurs systèmes de contrôle interne.

Face à l'évolution des environnements organisationnels, économiques et réglementaires, une révision majeure est opérée en 2013. Cette mise à jour donne naissance à COSO 2, qui intègre désormais les principes de la gestion des risques d'entreprise (*Enterprise Risk Management - ERM*), offrant ainsi une vision plus intégrée et holistique du pilotage des risques et du contrôle interne au service de la performance stratégique.

1.2.1. Définition et objectifs du contrôle interne

Le COSO définit le contrôle interne comme étant « *processus mis en œuvre par les dirigeants et le personnel d'une organisation destinée à assurer dans des limites raisonnables la réalisation des objectifs de l'optimisation des opérations, de la fiabilité des informations financières et de la conformité par rapport aux lois et aux règlements en vigueur* » (COSO 2013).

À ses origines, le contrôle interne avait une finalité principalement comptable et administrative. Il visait avant tout à mettre en place une organisation permettant un enregistrement fiable, exact et fidèle des opérations économiques et juridiques réalisées par l'entreprise, comme le souligne Mikol (1992, p. 46). Cette vision, centrée sur la rigueur documentaire et la traçabilité des flux, a progressivement évolué pour répondre aux exigences croissantes en matière de gouvernance, de transparence et de performance. Dans cette dynamique, « *La Nouvelle pratique du contrôle interne* » élargit le périmètre du contrôle interne en lui assignant quatre objectifs fondamentaux, qui en définissent aujourd'hui la portée moderne.

1.2.1.1. La sécurité des actifs

L'un des rôles fondamentaux du contrôle interne est d'assurer la protection des actifs de l'organisation. Ces actifs incluent non seulement les biens matériels (bâtiments, équipements, stocks, etc.), mais aussi les ressources immatérielles (brevets, bases de données, logiciels, savoir-faire, réputation) et humaines (compétences, expertise, personnel). Le système de contrôle interne doit mettre en place des dispositifs qui préviennent toute forme de perte, de vol, de détournement ou de dégradation, qu'elle soit intentionnelle (fraude, malveillance) ou accidentelle (erreur, négligence). Cela passe par des mesures de sécurisation physique et informatique, des procédures d'autorisation et de validation, des outils de suivi des accès et des responsabilités clairement définies. La sécurisation des actifs est également essentielle à la pérennité de l'entreprise, car toute atteinte à ces ressources peut engendrer des pertes financières, nuire à l'image de marque ou compromettre la continuité d'activité.

1.2.1.2. La fiabilité des informations recueillies

Le deuxième objectif du contrôle interne vise à garantir la fiabilité, la pertinence, la complétude et la rapidité des informations produites et diffusées au sein de l'organisation. Une information de qualité est essentielle pour une bonne gouvernance, une prise de décision efficace et une communication transparente avec les parties prenantes internes (direction, opérationnels, salariés) comme externes (investisseurs, autorités, partenaires). Le contrôle interne doit ainsi veiller à la qualité des données, à la rigueur des traitements comptables et financiers, à la cohérence des rapports, et à l'intégrité des systèmes d'information. Cela implique aussi la mise en place de mécanismes de validation, de contrôles croisés, d'archivage sécurisé et de traçabilité des opérations. Une information altérée, incomplète ou erronée peut engendrer des erreurs de pilotage, des décisions inadaptées, ou encore des sanctions réglementaires.

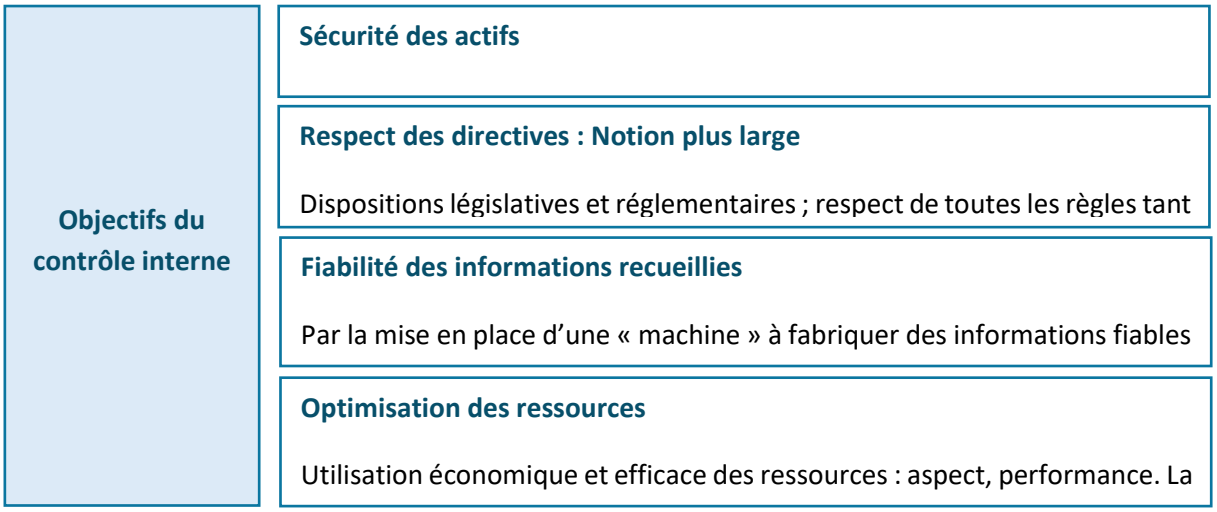
1.2.1.3. Le respect des directives

Ce troisième objectif renvoie à la conformité de l'organisation vis-à-vis des règles qui lui sont applicables. Cela inclut d'une part les dispositions légales et réglementaires imposées par les lois nationales, les normes sectorielles ou les régulateurs, et d'autre part les règles internes telles que les politiques de gouvernance, les procédures opérationnelles ou les codes de conduite. Le système de contrôle interne doit assurer que ces directives sont bien connues, comprises et appliquées à tous les niveaux de l'organisation. Cela suppose un travail d'information, de formation, de documentation, mais aussi un suivi des écarts, des sanctions en cas de non-respect, et des mécanismes d'alerte. Le non-respect de ces directives peut exposer l'entreprise à des risques juridiques, financiers ou réputationnels.

1.2.1.4. L'optimisation des ressources

Le dernier objectif du contrôle interne concerne la recherche d'une utilisation optimale des ressources disponibles. Il ne s'agit pas uniquement de maîtriser les coûts, mais d'assurer une efficacité (atteindre les objectifs fixés) et une efficience (atteindre ces objectifs avec un minimum de moyens ou avec le meilleur rendement possible) dans la mobilisation des ressources de l'entreprise. Cela concerne les ressources financières (budgets, investissements), humaines (répartition des tâches, développement des compétences), matérielles (utilisation des outils et équipements), informationnelles (exploitation des données), et structurelles (organigramme, circuits de décision). Le contrôle interne, dans ce cadre, aide à éviter les gaspillages, les redondances, les surcharges, tout en renforçant la performance globale de l'organisation.

Figure 1 : Objectifs du contrôle interne



Source : Eustache, 2015

1.2.2. Les composants du contrôle interne selon COSO

Le contrôle interne est décomposé par le référentiel COSO en cinq composants :

- L'environnement de contrôle ;
- L'évaluation des risques ;
- Les activités de contrôle ;
- L'information et la communication ;
- Le pilotage et surveillance.

1.2.2.1. L'environnement de contrôle

Selon le cadre COSO, l'environnement de contrôle est considéré comme « *un élément très important de la culture d'une entreprise, puisqu'il détermine le niveau de sensibilisation du personnel au besoin de contrôle. Il constitue le fondement de tous les autres éléments du contrôle interne, en imposant discipline et organisation* » (COSO, 1992).

L'environnement de contrôle constitue donc la pierre angulaire du système de contrôle interne. Il reflète l'attitude, la sensibilisation et les actions de la direction et de la gouvernance vis-à-vis du contrôle et de la gestion des risques. En d'autres termes, il définit le « *ton donné par le haut* » et influence la culture organisationnelle dans laquelle les activités de contrôle prennent place IIA, IFACI, 2015). Un environnement de contrôle solide crée les conditions nécessaires pour qu'un système de contrôle efficace puisse être mis en œuvre, en instaurant des normes d'éthique, d'intégrité et de comportement attendu au sein de l'organisation (Vanstapel Fr, 2004).

1.2.2.2. Évaluation des risques

L'évaluation des risques constitue une étape fondamentale du contrôle interne. Elle permet d'identifier, d'analyser et de hiérarchiser les événements susceptibles d'avoir un impact négatif sur la réalisation des objectifs de l'organisation (COSO, PWC, IFACI, 2014). Cette démarche proactive vise à anticiper les menaces, qu'elles soient d'origine interne ou externe, et à en apprécier la probabilité et les conséquences (Stringer et Carey, 2002). En fonction de cette analyse, l'entreprise peut mettre en place des mesures appropriées pour limiter ou maîtriser ces risques. Ce processus d'évaluation doit être régulièrement mis à jour afin de tenir compte des évolutions du contexte, des changements organisationnels et des nouveaux enjeux stratégiques.

1.2.2.3. Activité de contrôle

Le référentiel COSO définit ces activités comme étant « *l'application des normes et procédures destinées à assurer l'exécution des directives émises par le management en vue de maîtriser les risques. Ces activités sont menées à tous les niveaux hiérarchiques et fonctionnels de la structure et comprennent des actions aussi variées qu'approuver et autoriser, vérifier et rapprocher, apprécier les performances opérationnelles, la sécurité des actifs ou la séparation des fonctions* » (COSO, 1992).

Dans le cadre du contrôle interne, les activités de contrôle regroupent l'ensemble des procédures, des règles et des mécanismes mis en place pour s'assurer que les décisions prises par l'entreprise sont correctement exécutées et que les risques identifiés sont maîtrisés. Ces activités peuvent être préventives ou détectives, automatisées ou manuelles, et sont intégrées à tous les niveaux de l'organisation. Elles jouent un rôle essentiel dans l'atteinte des objectifs stratégiques, qu'il s'agisse de la performance opérationnelle, de la qualité et la fiabilité des informations financières, ou encore du respect des obligations légales et réglementaires (Cappelletti L, 2004).

1.2.2.4. Information et communication

D'après le référentiel COSO « *les systèmes d'information produisent, entre autres, des données opérationnelles financières ou encore liées au respect des obligations légales et réglementaires, qui permettent de gérer et contrôler l'activité. Ces systèmes traitent non seulement les données produites par l'entreprise mais également celles qui, liées à son environnement externe, sont nécessaires à la prise de décision pertinente comme au reporting externe* » (COSO, 1992).

Un système de contrôle interne efficace repose sur une circulation fluide et structurée de l'information. Il est essentiel que les données pertinentes soient accessibles aux bonnes personnes, au bon moment, et présentées de manière claire pour leur permettre de prendre des décisions éclairées et d'exercer les contrôles qui leur incombent (Rittenberg, 2006). La communication ne doit pas se limiter à une diffusion descendante, elle doit également permettre

des remontées d'information du terrain vers la direction, ainsi que des échanges transversaux entre les différentes fonctions de l'organisation. Cette dynamique favorise une meilleure coordination, une réactivité accrue face aux risques, et renforce la responsabilisation à tous les niveaux.

1.2.2.5. Le pilotage et surveillance

Le contrôle interne doit faire l'objet d'un suivi continu pour garantir sa pertinence et son efficacité dans le temps. Cette surveillance repose à la fois sur des mécanismes intégrés au quotidien et sur des revues périodiques, permettant d'identifier rapidement les défaillances ou les écarts éventuels. Le pilotage englobe l'ensemble des processus de l'organisation, y compris ceux confiés à des prestataires externes (IIA, IFACI, 2015). Il s'appuie notamment sur des indicateurs de performance, des retours d'expérience et l'intervention de dispositifs indépendants comme l'audit interne. Ce dispositif de veille contribue à l'amélioration continue du système, en l'adaptant aux évolutions internes et externes.

2. Cadre théorique de la recherche

Afin de mieux appréhender l'impact de la transformation digitale sur le contrôle interne, il convient de s'appuyer sur un cadre théorique solide permettant d'analyser les relations entre les technologies émergentes et ce dispositif de contrôle interne. Cette deuxième partie présente les fondements théoriques mobilisés dans cette recherche. Elle s'articule autour de deux approches complémentaires, à savoir la théorie de la contingence et la théorie de l'automatisation cognitive.

2.1. La théorie de la contingence

La théorie de la contingence, développée à partir des années 1960, postule qu'il n'existe pas de modèle unique de management ou de contrôle qui soit optimal pour toutes les entreprises. Au contraire, l'efficacité organisationnelle dépend d'un alignement entre les caractéristiques internes de l'organisation (telles que sa structure, ses processus, ou son système de contrôle interne) et les facteurs contextuels externes, tels que l'environnement technologique, le degré d'incertitude, la taille de l'entreprise ou son secteur d'activité (Lawrence et Lorsch, 1967).

Dans le contexte de la transformation digitale, cette approche permet de comprendre comment les entreprises ajustent leur dispositif de contrôle interne en fonction de la complexité croissante de leur environnement numérique (Burns et Stalker, 1961). L'introduction de technologies telles que l'IA, l'automatisation des processus (RPA), ou les ERP, modifie les flux d'information, les risques, et les modes de supervision. Cela oblige les entreprises à adapter leur système de contrôle pour rester efficace et pertinent.

Ainsi, à la lumière de la théorie de la contingence, le contrôle interne ne peut être envisagé de manière standardisée. Il doit au contraire être reconfiguré en fonction des caractéristiques

propres à chaque organisation et de son degré de maturité digitale. Une entreprise très digitalisée nécessitera par exemple des mécanismes de contrôle plus automatisés, des indicateurs en temps réel, et des systèmes de cybersécurité renforcés, là où une entreprise encore peu engagée dans la digitalisation pourra continuer à s'appuyer sur des dispositifs plus traditionnels.

En somme, la théorie de la contingence nous invite à considérer le contrôle interne non comme un système figé, mais comme un levier stratégique évolutif, qui doit s'aligner en permanence avec le contexte digital et les réalités opérationnelles de chaque organisation.

2.2. La théorie de l'automatisation cognitive

Dans un environnement économique marqué par une accélération de la transformation digitale, la théorie de l'automatisation cognitive constitue un cadre conceptuel pertinent pour comprendre les mutations actuelles du contrôle interne. Cette théorie permet d'éclairer les changements profonds qui affectent les systèmes de contrôle interne. Cette théorie repose sur l'idée que certaines fonctions cognitives humaines, telles que l'analyse, la prise de décision, la détection d'anomalies ou l'évaluation des risques, peuvent désormais être partiellement ou totalement automatisées grâce à des technologies avancées (Kaplan & Haenlein, 2019).

Les outils fondés sur l'intelligence artificielle, le machine learning ou encore le traitement automatique du langage naturel (NLP) sont capables de traiter de grandes quantités de données en temps réel, d'identifier des schémas invisibles à l'œil humain et de proposer des recommandations ou alertes intelligentes, facilitant ainsi la prise de décision. Appliquée au contrôle interne, cette approche transforme les processus classiques, souvent manuels et répétitifs, en mécanismes intelligents et proactifs.

En articulation avec la théorie de la contingence, la théorie de l'automatisation cognitive vient approfondir la réflexion sur l'adaptabilité du contrôle interne.

Tandis que la contingence insiste sur l'alignement du système de contrôle avec l'environnement externe, l'automatisation cognitive souligne l'importance de réinventer les modes de contrôle en tirant parti des innovations technologiques. Les entreprises qui parviennent à combiner ces deux logiques (adaptation contextuelle et intégration technologique) sont mieux positionnées pour répondre aux exigences de réactivité, de fiabilité et de performance dans un monde digitalisé.

3. Impact de la transformation digitale sur le dispositif de contrôle interne

Parmi les nombreux effets induits par la transformation digitale, son impact sur la qualité du contrôle interne constitue un enjeu central pour les organisations. En effet, l'intégration croissante des

technologies numériques modifie profondément la manière dont les dispositifs de contrôle sont conçus, mis en œuvre et évalués. Pour en apprécier pleinement la portée, il est pertinent d'analyser cette évolution à travers le cadre de référence du COSO, qui structure le contrôle interne autour de cinq composantes interdépendantes : l'environnement de contrôle, l'évaluation des risques, les activités de contrôle, l'information et la communication, ainsi que le pilotage. Cette grille d'analyse permet de présenter comment la digitalisation transforme chacun de ces volets. Les effets de la transformation numérique sur la qualité du contrôle interne se reflètent principalement dans les aspects suivants :

3.1. L'environnement de contrôle

L'environnement de contrôle constitue le socle culturel et organisationnel du dispositif de contrôle interne. Il reflète la philosophie de gestion de l'organisation, l'attitude de la direction face aux risques, et l'engagement de l'entreprise à respecter les normes éthiques et professionnelles. Avec la transformation digitale, cet environnement subit une mutation profonde. Ce changement ne se limite pas à l'adoption d'outils, mais touche à la manière même dont l'organisation conçoit le travail, le management et la gouvernance.

L'entrée dans l'ère du numérique oblige les entreprises à adapter leur stratégie et leur environnement de contrôle interne pour mieux répondre aux défis posés par l'arrivée de nouveaux entrants (Bloom, et al., 2013). Cela passe par des changements dans la structure organisationnelle, la culture d'entreprise et la politique de gestion des ressources humaines. Le modèle hiérarchique traditionnel laisse place à des structures plus horizontales, favorisant une plus grande autonomie et réactivité des employés. La transformation numérique facilite l'accès à l'information et réduit les coûts de transmission, ce qui permet une gestion plus autonome et une meilleure circulation des informations à tous les niveaux (Kretschmer et Khashabi. 2020). Ce processus génère également de nouvelles tâches et rend obsolètes certaines anciennes, orientant l'entreprise vers un modèle d'organisation apprenante. Enfin, la transformation numérique encourage une culture orientée vers les données, où les décisions sont de plus en plus guidées par l'analyse de données, renforçant ainsi l'efficacité et la qualité de l'environnement de contrôle interne (Sousa et Rocha, 2019).

3.2. L'évaluation des risques

L'identification et l'évaluation des risques constituent une composante structurante du contrôle interne, intervenant une fois que l'environnement de contrôle est en place. Cette étape repose sur la nécessité, pour toute organisation, de définir clairement ses objectifs afin de détecter les événements ou situations susceptibles d'en compromettre la réalisation. Elle implique un travail approfondi de recensement des sources potentielles de risques, qu'elles soient internes ou externes, suivi d'une analyse de leur probabilité et de leur impact. Selon le cadre conceptuel proposé par le COSO (2013), la gestion des

risques ne peut être dissociée du contrôle interne, tant elle en constitue une fonction essentielle et transversale (PWC & IFACI, 2014).

Traditionnellement, l'évaluation des risques reposait sur des méthodes qualitatives, souvent périodiques, mobilisant des matrices de risques, des jugements d'experts, et des entretiens manuels. Si ces approches permettaient une vision globale, elles restaient statiques, dépendantes de l'expérience humaine, et parfois inadaptées face à des environnements en rapide évolution (Shim et al., 2012). Avec la transformation digitale, l'évaluation des risques connaît une mutation structurelle. Les outils numériques, tels que l'analyse prédictive, l'intelligence artificielle ou encore le machine learning, permettent aujourd'hui de traiter d'importants volumes de données internes et externes en temps réel (Zou, et al., 2017). Cela favorise une identification plus rapide, plus fine et plus objective des risques, là où les méthodes anciennes pouvaient être biaisées ou lentes à réagir. Par exemple, des algorithmes peuvent désormais détecter des anomalies comportementales dans les opérations, anticiper des ruptures de chaîne logistique ou encore évaluer la solvabilité d'un partenaire avant même la signature d'un contrat. De plus, les technologies d'automatisation facilitent la mise à jour continue de la cartographie des risques, rendant l'exercice beaucoup moins dépendant de revues annuelles ou semestrielles (Thach et al., 2021). Cette transformation permet également une meilleure visualisation des risques grâce à des tableaux de bord interactifs, facilitant la prise de décision par les responsables opérationnels comme par les comités de direction.

3.3. Les activités de contrôle

Les activités de contrôle sont les actions qui permettent de garantir que les directives de la direction sont appliquées conformément aux politiques et procédures établies. La transformation numérique améliore considérablement l'efficacité de l'attribution des tâches aux employés. Grâce aux systèmes de gestion des RH numériques, les responsabilités sont clairement définies lors de la prise de décision, permettant ainsi à chacun d'assumer la responsabilité de ses actes et de mieux remonter aux tâches non exécutées. (Huidong, 2023).

Les activités de contrôle, historiquement manuelles et périodiques, deviennent aujourd'hui automatisées, grâce à l'intégration d'outils Robotic Process Automation (RPA) qui exécutent des tâches de contrôle répétitives sans intervention humaine, ces activité devient également intelligentes, via l'utilisation d'outils d'intelligence artificielle capables de détecter des anomalies ou des tendances à partir de vastes volumes de données, et devient des activités intégrées aux processus opérationnels, grâce à des ERP évolués qui embarquent directement les contrôles dans les workflows métiers. Cela permet un renforcement de l'efficacité et une réduction des erreurs humaines.

3.4. L'information et la communication

La composante « *information et communication* » du contrôle interne repose sur la capacité d'une organisation à produire, diffuser et utiliser une information pertinente, fiable et en temps opportun. La transformation digitale a profondément remodelé ce volet, en rendant les échanges d'informations plus efficaces, plus structurés et moins dépendants des chaînes hiérarchiques traditionnelles. Les outils numériques permettent aujourd'hui une circulation fluide de l'information entre les différentes fonctions, niveaux hiérarchiques et entités de l'organisation. Des solutions comme les ERP intégrés, les plateformes collaboratives, ou encore les systèmes de gestion documentaire facilitent un accès instantané aux données clés pour toutes les parties prenantes concernées. Là où auparavant l'information était souvent cloisonnée, incomplète ou transmise avec délai, elle devient désormais largement disponible, actualisée en continu et centralisée dans des systèmes interconnectés.

Cette amélioration n'impacte pas seulement la rapidité des échanges, mais aussi leur qualité : les messages sont mieux ciblés, les données sont plus traçables, et les risques de distorsion sont considérablement réduits. En parallèle, la communication interne évolue vers un modèle plus horizontal et interactif, favorisant la remontée d'informations terrain, la collaboration transversale, et l'alignement stratégique.

Sur le plan externe, la digitalisation renforce également la capacité des entreprises à répondre aux exigences de transparence et de conformité, en facilitant la communication avec les auditeurs, les régulateurs et les parties prenantes via des interfaces numériques sécurisées.

L'adoption des technologies numériques contribue à une diminution significative des coûts opérationnels, notamment en réduisant les frais liés à la communication entre les différentes implantations géographiques de l'entreprise. Des outils comme la visioconférence et le travail à distance se sont largement généralisés, remplaçant les échanges physiques par des interactions virtuelles efficaces. En éliminant les contraintes de distance et de temps, la transformation digitale favorise une circulation plus rapide et plus homogène de l'information au sein de l'organisation (Huidong, 2023).

3.5. Les activités de supervision et de pilotage

Dans un environnement en constante évolution, la capacité des entreprises à surveiller et ajuster leurs dispositifs de contrôle interne de manière continue devient essentielle. La transformation numérique apporte à cet égard des outils puissants qui renforcent considérablement l'efficacité des activités de pilotage. Grâce à l'automatisation et à la numérisation des processus, il est désormais possible d'intégrer des mécanismes de suivi directement au cœur des opérations quotidiennes. Cela permet une détection rapide des anomalies, une réaction quasi instantanée face aux dysfonctionnements, et un ajustement en temps réel des contrôles. Contrairement aux approches traditionnelles qui reposaient souvent sur des contrôles périodiques ou ponctuels, les dispositifs actuels s'appuient sur des flux de données continus,

facilitant une surveillance proactive et étendue. Les outils d'analyse avancée, comme le Big Data et les algorithmes d'apprentissage automatique, permettent aux auditeurs internes d'examiner l'ensemble des données disponibles, au lieu de se limiter à des échantillons, ce qui améliore significativement la précision et la portée des audits (Huidong, 2023).

Par ailleurs, en réduisant l'asymétrie d'information entre les dirigeants et les actionnaires, les technologies numériques renforcent la transparence et soutiennent un meilleur alignement des intérêts dans les relations de gouvernance. La surveillance devient ainsi un levier de pilotage stratégique, offrant aux organes de direction et aux conseils d'administration une visibilité accrue sur la performance des contrôles et sur les risques résiduels (Manita et al., 2019). En centralisant les informations issues des systèmes interconnectés, la transformation digitale permet d'optimiser la prise de décision, de prévenir les dérives comportementales, et de renforcer globalement la qualité du contrôle interne.

CONCLUSION

La transformation digitale, en s'inscrivant au cœur des dynamiques organisationnelles contemporaines, impacte de manière transversale les cinq composantes du contrôle interne telles que définies par le référentiel COSO. Elle renforce l'environnement de contrôle en facilitant la diffusion de la culture du risque à travers des outils collaboratifs et des plateformes d'échange. Elle améliore l'évaluation des risques grâce à l'analyse prédictive et au traitement massif de données en temps réel. Les activités de contrôle bénéficient de l'automatisation, qui permet une exécution plus rapide, plus fiable et moins sujette aux erreurs humaines. L'information et la communication sont également transformées, avec des systèmes intégrés favorisant une circulation fluide et sécurisée des données. Enfin, le pilotage et la surveillance du dispositif est renforcé par des tableaux de bord dynamiques et des outils d'audit en continu, permettant un suivi proactif et permanent des opérations.

Néanmoins, en dépit des nombreux bénéfices qu'elle procure, la transformation digitale soulève également de nouveaux défis, notamment en matière de cybersécurité et de gestion des données sensibles. Si les technologies numériques offrent un renforcement certain des dispositifs de contrôle interne, elles ne peuvent se substituer entièrement à l'intuition, au discernement et à l'expertise humaine, indispensables à l'analyse de situations complexes et à la prise de décision dans des environnements incertains. Dès lors, l'efficacité du contrôle interne à l'ère digitale repose sur une complémentarité entre les apports de l'automatisation et l'intervention humaine, où la technologie joue un rôle d'outil de soutien, sans pour autant remplacer le jugement professionnel.

La transformation digitale offre aux entreprises marocaines une opportunité stratégique pour renforcer leur contrôle interne. Pour en tirer pleinement parti, il est essentiel que ces entreprises investissent dans la formation continue de leurs équipes afin de maîtriser les outils numériques, tout en adoptant des solutions technologiques adaptées telles que les ERP, l'IA ou la blockchain pour automatiser les processus. Une gouvernance numérique renforcée, associée à des politiques de sécurité strictes, garantira la protection des données et l'intégrité des systèmes. Il est également crucial d'encourager une culture de la gestion des risques et de la conformité, notamment en intégrant la cybersécurité dans les stratégies globales. Enfin, la collaboration avec des experts externes, en matière de cybersécurité et d'audit, sera un atout majeur pour réussir cette transformation et améliorer l'efficacité du contrôle interne.

Références

(1) Bloom N., Garicano L., Sadun R., Reenen J.V. The Distinct Effects of Information Technology and Communication Technology on Firm Organization. Management Science 2014, doi:10.1287/mnsc.2014.2013.

(2) Bloching, B., Leutiger, P., Oltmanns, T., & Rossbach, C. (2015). The digital transformation of industry -How important is it? Who are the winners? What must be done? A European study commissioned by the Federation of German Industries (BDI) and conducted by Roland Berger Strategy Consultants, 1-52.

(3) Bowersox DJ, Closs DJ, Drayer RW (2005) The digital transformation: technology and beyond. Supply Chain Manag Rev 9(1):22–29.

(4) COSO. (2013). Internal Control — Integrated Framework. Committee of Sponsoring Organizations of the Treadway Commission.

(5) COSO, PWC, IFACI. (2014), Référentiel intégré de contrôle interne : Application au reporting financier externe, Paris, Eyrolles.

(6) CAPPELLETTI, L. (2004). Vers une institutionnalisation de la fonction contrôle interne ?. comptabilité – contrôle – audit / Tome 12 – Volume 1 (p. 27 à 43).

(7) Eustache Ebondo Wa Mandzila (2004). la contribution du contrôlé interne et de l'audit au gouvernement d'entreprise. Gestion et management. Université paris.

(8) Fitzgerald et al. (2013). Embracing Digital Technology, MIT Sloan Management. Review, 1-12.

(9) Huidong M., (2023). The Impact of Digital Transformation on Internal Control Quality: A Study Based on Five Components of Internal Control. Accounting and Corporate Management, 28-34. DOI: 10.23977/acccm.2023.050405.

(10) Hanelt et al., (2021). "A Systematic Review of the Literature on Digital Transformation: Insights and Implications for Strategy and Organizational Change," Journal of Management Studies, Wiley Blackwell, vol. 58(5), pages 1159-1197, July.

(11) IFACI. (2020). Le contrôle interne à l'ère du numérique. Institut Français de l'Audit et du Contrôle Interne.

(12) IIA, IFACI. (2015), Manuel d'audit interne : Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques, Eyrolles, Chapitre 4.

(13) Kretschmer T., Khashabi P. Digital Transformation and Organization Design: An Integrated Approach. California Management Review 2020, 62, 86–104, doi:10.1177/0008125620940296.

(14) LOULID A. et HEFNAWI I., (2021). « Enjeux, défis et impact de la transformation digitale : une revue systématique de la littérature. Journal of business and economics. Volume 11 N° 1 & 2. 115-131.

(15) Manita R., Elommal N., Baudier P., Hikkerova L. The Digital Transformation of External Audit and Its Impact on Corporate Governance. Technological Forecasting and Social Change 2020, 150, 119751, doi: 10. 1016/ j. techfore. 2019. 119751.

(16) Mazzone, D. M. (2014). Digital or Death: Digital Transformation: The Only Choice for Business to Survive. Smashbox Consulting Inc.

(17) Shim C.-S., Lee K.-M., Kang L.S., Hwang J., Kim Y. Three-Dimensional Information Model-Based Bridge Engineering in Korea. Structural Engineering International 2012, 22, 8–13, doi:10.2749/101686612X13216060212834.

(18) Solis B., Lieb R., Szymanski J. (2014). The 2014 state of digital transformation. Altimeter Group.

(19) Stringer. C, Carey. P. (2002), Internal Control Re-Design: An Exploratory Study of Australian Organisations, University of Otago, Monash University.

(20) Sousa M.J., Rocha Á. Digital Learning: Developing Skills for Digital Transformation of Organizations. Future Generation Computer Systems 2019, 91, 327–334, doi:10.1016/j.future.2018.08.048.

(21) Thach N.N., Hanh H.T., Huy D.T.N., Vu Q.N (2021). Technology Quality Management of the Industry 4.0 and Cybersecurity Risk Management on Current Banking Activities in Emerging Markets-the Case in Vietnam. International Journal for Quality Research, 15, 845.

(22) Verhoef et al., (2021). "Digital transformation: A multidisciplinary reflection and research agenda," Journal of Business Research, Elsevier, vol. 122(C), pages 889-901.

(23) Vanstapel FR. (2004), Lignes directives sur les normes de contrôle interne à promouvoir dans le secteur public, INTOSAI, Bruxelles.

(24) Zou Y., Kiviniemi A., Jones S.W. A Review of Risk Management through BIM and BIM-Related Technologies. Safety Science 2017, 97, 88–98, doi:10.1016/j.ssci.12.027.