# Management des risques des SI au Maroc : Entre ambition réglementaire et défis culturels -Une analyse critique de l'état des lieux

Hajar Belhaj, Said Kammas, Youssef Al Meriouh

ISSN: 2658-8455
Volume 5, Issue 10 (2024), pp. 317-346.


IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

# Management des risques des SI au Maroc : Entre ambition réglementaire et défis culturels - Une analyse critique de l'état des lieux

# IS Risk Management in Morocco: Between regulatory ambitions and cultural challenges - A critical analysis of the current situation

**Hajar BELHAJ, *(Doctorant)***
*École Nationale de Commerce et de Gestion de Tanger*
*Université Abdelmalek Essaadi, Maroc*

**Said KAMMAS, *(Enseignant-Chercheur)***
*Centre de Recherches et Études en Logistique et Développement, Maroc*
*PhD, Enseignant-Chercheur en sciences de management, Consultant CMC®, Auditeur QHSEE&SI*

**Youssef AL MERIOUH, *(Enseignant-Chercheur)***
*École Nationale de Commerce et de Gestion de Tanger*
*Université Abdelmalek Essaadi, Maroc*

| | |
|---|---|
| **Adresse de correspondance :** | Route de l'aéroport, B.P 1255<br>B.P : 90000 Tanger, Maroc<br>Tél. +212 (0) 539 313 4 87<br>Tél. +212 (0) 539 313 4 88<br>Email : encgtanger@encgt.ma |
| **Déclaration de divulgation :** | Les auteurs n'ont pas connaissance de quelconque financement qui pourrait affecter l'objectivité de cette étude et ils sont responsables de tout plagiat dans cet article. |
| **Conflit d'intérêts :** | Les auteurs ne signalent aucun conflit d'intérêts. |
| **Citer cet article** | BELHAJ, H., KAMMAS, S., & AL MERIOUH, Y. (2024). Management des risques des SI au Maroc : Entre ambition réglementaire et défis culturels - Une analyse critique de l'état des lieux. *International Journal of Accounting, Finance, Auditing, Management and Economics*, *5*(10), 317-346. https://doi.org/10.5281/zenodo.13909392 |
| **Licence** | **Cet article est publié en open Access sous licence CC BY-NC-ND** |

*Received: August 29, 2024* *Accepted: October 07, 2024*

ISSN: 2658-8455
Volume 5, Issue 10 (2024), pp. 317-346.


IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

# Management des risques des SI au Maroc : Entre ambition réglementaire et défis culturels - Une analyse critique de l'état des lieux

**Résumé :**

Cette étude dresse un état des lieux critique du management des risques des systèmes d'information (SI) au Maroc, en examinant l'interaction entre le cadre réglementaire, les normes nationales et les facteurs culturels et organisationnels. L'objectif est d'évaluer l'efficacité du dispositif actuel et d'identifier les défis spécifiques au contexte marocain. La méthodologie s'appuie sur une analyse documentaire approfondie des textes législatifs, des référentiels nationaux et des publications scientifiques, complétée par une analyse comparative avec les standards internationaux. Les résultats révèlent un cadre réglementaire ambitieux mais une adoption limitée des pratiques de gestion des risques SI, notamment dans les PME. L'étude met en lumière l'influence significative des facteurs culturels, tels que l'attitude vis-à-vis du risque et la résistance au changement, sur l'implémentation effective des stratégies de gestion des risques SI. Ces constats soulignent la nécessité d'adapter les approches de gestion des risques au contexte local et d'intensifier les efforts de sensibilisation et de formation pour améliorer la maturité du management des risques SI au Maroc.

**Mots-clés :** Management des risques SI, Cybersécurité au Maroc, Cadre réglementaire, Gouvernance des SI, Facteurs culturels
**Classification JEL :** M15 ; G32
**Type d'article :** Recherche exploratoire

**Abstract:**

This study critically assesses Information Systems (IS) risk management in Morocco, examining the interactions between the regulatory framework, national standards, and cultural and organizational factors. The objective is to evaluate the current system's effectiveness and identify challenges specific to the Moroccan context. The methodology relies on an in-depth documentary analysis of legislative texts, national guidelines, and scientific publications, complemented by a comparative analysis with international standards. The results reveal an ambitious regulatory framework but a limited adoption of IS risk management practices, particularly among SMEs. The study highlights the significant influence of cultural factors, such as attitude to risk and resistance to change, on implementing IS risk management strategies effectively. These findings underscore the need to adapt risk management approaches to the local context and intensify awareness and training efforts to improve the maturity of IS risk management in Morocco.

**Keywords:** IS Risk Management, Cybersecurity in Morocco, Regulatory Framework, IS Governance, Cultural Factors
**JEL Classification:** M15; G32
**Paper type:** Exploratory Research

ISSN: 2658-8455
Volume 5, Issue 10 (2024), pp. 317-346.

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

## 1. Introduction

Dans un contexte de transformation numérique accélérée, le management des risques des systèmes d'information (SI) est devenu un enjeu crucial pour les organisations du monde entier (Siponen, 2000). D'ailleurs, la mondialisation économique a fait émerger de nouvelles dimensions de risque qui étaient jusque-là peu explorées. Désormais, quel que soit la taille ou l'impact des organisations socio-économiques, la pérennité de ces dites organisations, est une variable aléatoire au sein d'un système d'équations caractérisé par sa complexité et la diversité de ses facteurs hétérogènes difficilement maîtrisables. Par conséquent, l'entreprise contemporaine doit s'inscrire dans une approche d'amélioration continue de sa performance, par l'innovation et la proposition d'une qualité de service distinguable et reconnaissable aux marchés locaux, régionaux, nationaux et internationaux. En effet, dans cette course à la continuité et à la pérennité, le moindre risque imprévu peut mettre en péril même l'intégrité de l'organisation (Mazouni, 2008).

Le paysage économique mondial, subit une transformation radicale sous l'impulsion des technologies de l'information (TI). Une adoption massive des TI par les entreprises démontre leur rôle central dans la transformation des modèles économiques et des processus opérationnels (Laudon & Laudon, 2020).

Cependant, cet engouement croissant est accompagné de plusieurs défis imposés à la gestion des risques des systèmes d'information. L'un des principaux défis est la nature volatile des cybermenaces, et l'intensification de leurs fréquences dans les derniers temps. Selon une étude de Symantec publiée en 2024[1], les ransomwares restent l'une des formes les plus lucratives de la cybercriminalité et, à ce titre, constituent une menace endémique pour les organisations de toutes tailles, engendrant des graves perturbations. Dans leur rapport sur le paysage des cybermenaces de l'année 2023, ils ont exposé une escalade aggravée et ont souligné que les attaques ayant presque doublé par rapport à octobre 2022. Les attaquants évoluent continuellement leurs tactiques et exploitent les vulnérabilités connues dans les applications publiques tels que Microsoft Exchange Server et Citrix NetScaler.[2]

Dans la même vision, l'intégration de la technologie ne propose pas que des opportunités d'amélioration, mais elle entrave des nouvelles vulnérabilités. L'adoption de technologies comme l'informatique en nuage, l'internet des objets (IdO) et l'intelligence artificielle (IA), présente des opportunités indéniables, mais elle s'accompagne également de défis inédits. L'informatique en nuage, par exemple, offre une évolutivité et une rentabilité accrue, mais soulève des préoccupations en matière de sécurité et de confidentialité des données en raison de la nature partagée des environnements cloud (Subashini & Kavitha, 2011).

Le Maroc, en tant que pays émergent aspirant à se positionner comme un leader régional en matière de technologies de l'information, n'échappe pas à cette réalité (Chergui et al., 2016). Cependant, la gestion efficace des risques SI dans le contexte marocain présente des défis uniques liés à des facteurs réglementaires, culturels et organisationnels spécifiques.

Au cours de la dernière décennie, le Maroc a déployé des efforts considérables pour renforcer sa résilience face aux cybermenaces, notamment par l'adoption d'une stratégie nationale de cybersécurité en 2013 et la mise en place d'un cadre réglementaire ambitieux (Hathaway & Spidalieri, 2018). Néanmoins, l'efficacité de ces initiatives et leur adoption par les organisations marocaines, en particulier les petites et moyennes entreprises (PME) qui constituent l'épine dorsale de l'économie du pays, restent à évaluer (Abaaoukide & Bentaleb, 2011).

[1] https://symantec-enterprise-blogs.security.com/threat-intelligence/ransomware-threat-landscape-2024 consulté le 20/06/2024

[2] https://hansesecure.de/en/2024/03/the-alarming-increase-in-cyber-attacks-why-every-business-is-at-risk/ consulté le 20/06/2024

ISSN: 2658-8455
Volume 5, Issue 10 (2024), pp. 317-346.

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

La littérature existante souligne l'importance de la culture organisationnelle dans l'adoption et la mise en œuvre efficace des pratiques de gestion des risques SI (Chang & Ho, 2006; Jackson, 2011). Dans le contexte marocain, caractérisé par une culture d'entreprise distincte et des attitudes spécifiques vis-à-vis du risque, il est crucial d'examiner comment ces facteurs culturels influencent le management des risques SI (Kadmiri et al., 2021).

Malgré l'importance croissante de ce sujet, il existe un manque de recherches approfondies sur l'état actuel du management des risques SI, prenant en compte à la fois le cadre réglementaire, les pratiques organisationnelles et les facteurs culturels. Cette étude vise à combler cette lacune en dressant un état des lieux critique et complet du management des risques SI au Maroc.

L'objectif principal de cette recherche est d'évaluer l'efficacité du dispositif actuel de gestion des risques SI et d'identifier les défis spécifiques au contexte marocain. Premièrement, cette étude vise à analyser le cadre réglementaire et normatif marocain en matière de gestion des risques SI. Cette analyse comprend une évaluation de la conformité de ce cadre avec les standards internationaux, permettant de mettre en lumière les éventuelles lacunes ou opportunités d'amélioration. Deuxièmement, l'enquête s'étend à l'examen du niveau d'adoption et de mise en œuvre des pratiques de gestion des risques SI au sein des entreprises marocaines, en accordant une attention particulière aux PME. Ces entités représentent un segment vital de l'économie marocaine mais sont souvent moins équipées pour faire face aux défis complexes des risques SI.

En outre, il est crucial d'identifier les facteurs culturels et organisationnels qui influencent l'efficacité du management des risques SI. Comprendre ces facteurs permettra de cerner les barrières et les leviers existants au sein des organisations marocaines en ce qui concerne la gestion des risques SI. Cette compréhension est indispensable pour adapter les pratiques de gestion au contexte marocain.

Enfin, sur la base des analyses précédentes, cette recherche proposera des recommandations stratégiques pour améliorer la maturité du management des risques SI dans les entreprises marocaines. Ces recommandations viseront à fournir des directives pratiques et théoriques pour renforcer la résilience et la réactivité des organisations face aux menaces informatiques croissantes.

Cette étude contribuera à l'enrichissement de la littérature existante en offrant une perspective unique sur les défis et les opportunités liés au management des risques SI dans un pays émergent, en mettant en lumière l'interaction complexe entre les cadres réglementaires, les pratiques organisationnelles et les facteurs culturels. Les résultats de cette recherche fourniront des perspectives précieuses pour les décideurs politiques, les dirigeants d'entreprises et les professionnels de la sécurité des SI au Maroc et dans d'autres pays émergents confrontés à des défis similaires.

## 2. Fondements théoriques de la gestion des risques des systèmes d'information

Le management des risques dans le contexte des systèmes d'information (SI) est un domaine qui a suscité l'intérêt de plusieurs chercheurs, donnant lieu à l'élaboration de nombreuses théories visant à expliquer et à structurer les pratiques de gestion des risques. Pour enrichir notre analyse documentaire, il est essentiel de comprendre les fondements théoriques qui encadrent ce champ d'étude. Ces théories offrent des cadres conceptuels permettant de mieux appréhender les enjeux, les dynamiques et les approches stratégiques pour atténuer les risques liés aux SI.

### 2.1. Théorie de la contingence

Cette théorie suggère que les stratégies de gestion des risques doivent être contextuelles et s'adapter aux facteurs contextuels internes et externes liés à l'adoption de la gestion des risques

ISSN: 2658-8455
Volume 5, Issue 10 (2024), pp. 317-346.

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

au sein des organisations. Parmi ces facteurs étudiés, nous trouvons l'influence des conseils d'administration (Desender, 2011), l'affiliation de l'industrie (Beasley et al., 2005), la taille de l'organisation (Pagach & Warr, 2011) et la pression réglementaire (Kleffner et al., 2003). Cependant, bien que quelques auteurs aient démontré l'impact de certains facteurs sur l'adoption des pratiques de la gestion des risques, d'autres trouvent que certains de ces facteurs tels que la taille de l'organisation et l'affiliation de l'industrie, ont des effets inexplicables (Mikes & Kaplan, 2014).

### 2.2. Théorie de la résilience organisationnelle

Thalassinos et al. (2023) ont postulé que la compréhension de la résilience diffère selon les disciplines et les contextes de recherche. Au vrai sens, la résilience organisationnelle consiste à préserver la valeur de l'entreprise dans un environnement perturbant, et de se transformer positivement suite aux crises inattendues (Vogus & Sutcliffe, 2007). Cette flexibilité vis-à-vis un environnement incertain, semble évidente pour les organisations dans des domaines tels que la gestion des risques, la gestion de la continuité des activités, et la cybersécurité pour se protéger dans le passé (Braes & Brooks, 2011). Ce dernier auteur a avancé également que la résilience organisationnelle est un processus à la fois descendant et ascendant, qui tient compte de la culture, des valeurs, de la direction de l'organisation et des processus fonctionnels tels que la gestion des risques et la sensibilisation.

### 2.3. Théorie des parties prenantes dans la gestion des risques

La littérature de la théorie des parties prenantes suppose que certains groupes et individus ont un intérêt dans le succès ou l'échec d'une entreprise (Freeman, 2010). D'ailleurs, Rana et al. (2019) ont argumenté que la compréhension des forces institutionnelles ou structurelles (lois, réglementations, cadres, politiques, bureaux, processus et procédures) est cruciale pour la compréhension du cadre de gestion des risques. Selon (Pradesa et al., 2021), certaines parties prenantes offrent des perspectives prometteuses, tandis que d'autres soulèvent de risques inquiétants. D'où vient la nécessité de la prise en compte de la signification des risques pour chaque principale partie prenante.

### 2.4. Théorie de l'agence

La théorie de l'agence s'intéresse principalement à l'étude des défis posés par la délégation de pouvoir d'un acteur à un autre (Zsidisin & Ellram, 2003). Osipova (2015) discute la gestion conjointe des risques entre les mandants et les mandataires et met en évidence l'importance du partage des risques dans les relations d'agence, pour assurer une collaboration solide. Il conclue donc qu'une gestion conjointe des risques qui est efficace, dépend fortement de la collaboration favorisée par des initiatives comme l'approvisionnement coopératif et la communication ouverte. Dans une autre perspective, le fait que la théorie d'agence traite des problèmes qui apparaissent dans les entreprises en raison de la séparation entre les propriétaires et les gestionnaires et met l'accent sur la réduction de ce problème. Les différences d'attitude à l'égard du risque entre le mandant et les agents, ont été investigués par plusieurs auteurs (Chowdhury, 2004; Lundqvist, 2015), et des nombreux déterminants ont été discutés tels que l'indépendance des membres du conseil d'administration (Miller, 2009) et la propriété managériale (Wellalage & Locke, 2011). Selon (Lundqvist, 2015), il est nécessaire donc d'avoir une structure de gouvernance solide pour une gestion efficace des risques, qui concilie les intérêts des dirigeants avec ceux des propriétaires.

### 2.5. Théorie de la complexité

Dans les théories traditionnelles, la causalité est linéaire : A entraîne B qui entraîne C. En revanche, la théorie de la complexité met en avant des interactions complexes et non linéaires,

ISSN: 2658-8455
Volume 5, Issue 10 (2024), pp. 317-346.

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

où les événements s'auto-influencent et co-évoluent en produisant le résultat final, même que si, ce résultat final ne peut pas être connu avec précision (Emblemsvåg, 2020). Dekker (2013) argumente que la complexité croissante de nos organisations et de leurs technologies a dépassé notre compréhension du succès ou d'échec des systèmes complexes. D'autre part, Nason (2017) postule que la gestion des risques ne se limite pas à l'audit et à l'application de listes de contrôle, et qu'elle peut s'avérer extrêmement difficile, même sans prendre en compte les effets de la complexité. Il affirme donc que l'approche holistique de la gestion des risques de l'entreprise (ERM) constitue une amélioration par rapport aux approches plus traditionnelles, axées seulement sur les fonctions.

### 2.6. Théorie de l'apprentissage organisationnel

Argyris & Schön (1997) étaient parmi les premiers à discuter l'importance de l'apprentissage organisationnel. Ils mettent en lumière la capacité de l'organisation à intégrer les erreurs, les incongruités et les incompatibilités dans une théorie d'action organisationnelle qui émerge nécessairement au fur et à mesure que le système organisationnel/environnemental évolue. Ils affirment également que les organisations sont très douées pour l'apprentissage en boucle unique, mais elles peuvent s'améliorer en intégrant l'apprentissage en double boucle (Argyris, 1977). Amien (2014) souligne que l'apprentissage organisationnel et les processus de gestion des risques dépendent de la manière dont il est configuré ou structuré dans l'organisation. Il conclue également le rôle important du cadre régissant la gestion des risques, présenté par diverses normes telles que l'ISO, dans la facilitation d'apprentissage dans l'organisation.
Après avoir établi les fondements théoriques liés à la gestion des risques des systèmes d'information, il est crucial d'examiner comment ces théories se traduisent dans le contexte spécifique du Maroc.

## 3. Contexte et cadre conceptuel

Au cours des deux dernières décennies, le Maroc a connu une transformation numérique significative, caractérisée par une adoption croissante des technologies de l'information et de la communication (TIC) dans tous les secteurs de l'économie. Selon (Chergui et al., 2016), cette évolution a été facilitée par l'ouverture du Maroc sur l'Europe et sa position géostratégique, lui permettant de se tenir informé des progrès technologiques et de les adopter progressivement.
L'adoption des systèmes d'information (SI) a particulièrement marqué le paysage des entreprises marocaines. Bighrissen & Cherkaoui (2012) ont noté une croissance significative de l'implantation des systèmes ERP (Enterprise Resource Planning) depuis plus d'une décennie, témoignant de l'investissement massif des entreprises dans ces systèmes d'envergure. Cette tendance s'observe tant dans le secteur privé que public, avec des implications financières et opérationnelles considérables (El Abbassi & Chafik, 2014). Cependant, cette évolution rapide s'accompagne de nouveaux défis, notamment en termes de sécurité et de gestion des risques liés aux SI. La complexité croissante des systèmes et l'interconnexion accrue des réseaux ont augmenté la vulnérabilité des organisations aux cybermenaces, rendant crucial le développement d'une approche structurée de management des risques SI.
Avant de poursuivre, il convient de noter que le management des risques des systèmes d'information se définit comme l'ensemble des processus permettant d'identifier, d'évaluer et de traiter les menaces potentielles pesant sur les actifs informationnels d'une organisation. Selon la norme ISO/IEC 27005, ce processus comprend plusieurs étapes clés :

- Établissement du contexte
- Identification des risques
- Analyse des risques
- Évaluation des risques

ISSN: 2658-8455
Volume 5, Issue 10 (2024), pp. 317-346.

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

- Traitement des risques

Ces étapes s'inscrivent dans un cycle continu d'amélioration, incluant la communication et la consultation avec les parties prenantes, ainsi que la surveillance et la revue régulière du processus.

Dans le contexte marocain, la compréhension et l'application de ces concepts sont essentielles pour développer une approche efficace de gestion des risques SI, adaptée aux spécificités locales. Le tissu économique marocain est caractérisé par une prédominance des PME (Abaaoukide & Bentaleb, 2011). Cette structure présente des défis particuliers en termes de management des risques SI, notamment en raison de ressources limitées et d'une sensibilisation parfois insuffisante aux enjeux de la sécurité informatique.

Par ailleurs, le contexte culturel marocain joue un rôle significatif dans l'approche du risque et de l'incertitude. Kadmiri et al. (2021) soulignent l'importance d'adapter les stratégies de gestion des risques aux spécificités locales pour encourager l'entrepreneuriat et le développement économique. Cette adaptation culturelle est primordiale pour assurer l'efficacité des pratiques de management des risques SI dans les organisations marocaines.

Enfin, le cadre réglementaire et institutionnel marocain en matière de cybersécurité et de protection des données a considérablement évolué ces dernières années, avec l'adoption de lois spécifiques et la création d'organismes dédiés. Ce contexte réglementaire en évolution rapide constitue à la fois un défi et une opportunité pour les organisations dans leur démarche de gestion des risques SI.

La compréhension de ces spécificités est essentielle pour appréhender les enjeux du management des risques SI au Maroc et pour analyser l'efficacité des approches actuelles. Elle servira de base pour l'examen détaillé du cadre réglementaire, des pratiques organisationnelles et des facteurs culturels qui seront abordés dans les sections suivantes de cette étude.

## 4. Méthodologie de recherche

Cette étude adopte une approche qualitative exploratoire pour dresser un état des lieux détaillé du management des risques des systèmes d'information au Maroc. Ce choix méthodologique se justifie par la nature complexe et multidimensionnelle du sujet, qui nécessite une analyse approfondie des contextes réglementaires, organisationnels et culturels (Yin, 2018).

La conception de la recherche s'articule autour d'une analyse documentaire exhaustive, complétée par une analyse comparative avec les standards internationaux. Cette approche permet d'obtenir une vue d'ensemble du paysage actuel du management des risques SI, tout en identifiant les spécificités et les défis propres au contexte national.

Ainsi, la collecte de données s'est effectuée à travers plusieurs sources :

a) Analyse documentaire :

- Textes législatifs et réglementaires marocains relatifs à la cybersécurité et à la protection des données
- Publications officielles de la Direction Générale de la Sécurité des Systèmes d'Information (DGSSI)
- Normes et référentiels publiés par l'Institut Marocain de Normalisation (IMANOR)
- Rapports gouvernementaux et études sectorielles sur la sécurité des SI au Maroc
- Articles scientifiques et publications académiques traitant du sujet dans le contexte marocain

b) Analyse comparative :

- Standards internationaux de gestion des risques SI (ISO 27001, NIST Cybersecurity Framework)

ISSN: 2658-8455
Volume 5, Issue 10 (2024), pp. 317-346.

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

- Rapports et études sur les pratiques de gestion des risques SI dans d'autres pays émergents

L'analyse des données a été réalisée selon une approche thématique (Braun & Clarke, 2006) permettant d'identifier les principales tendances, les défis récurrents et les facteurs spécifiques influençant le management des risques SI au Maroc. Une attention particulière a été portée à la triangulation des sources pour assurer la validité et la fiabilité des résultats.

Pour mieux appréhender cette analyse, les sources documentaires ont été sélectionnées selon leur pertinence par rapport au management des risques SI au Maroc, et leur crédibilité (publications académiques évaluées par les pairs, documents officiels, rapports d'organismes reconnus). Également, l'étude couvre la période de 2010 à 2024, permettant ainsi de saisir l'évolution récente du cadre réglementaire et des pratiques en matière de gestion des risques SI au Maroc.

Le processus de l'analyse des données a permis d'identifier, d'analyser et de rapporter les thèmes au sein des données collectées. Il est constitué de six phases : familiarisation avec les données, génération de codes initiaux, recherche de thèmes, révision des thèmes, définition et nomination des thèmes, et production du rapport (Braun & Clarke, 2006).

La comparaison avec les standards internationaux a été effectuée en utilisant une grille d'analyse comparative. Cette grille a été élaborée à partir des principaux éléments des standards ISO 27001 et du NIST Cybersecurity Framework. Chaque aspect du cadre marocain a été évalué en termes de présence/absence et de degré d'alignement avec ces standards internationaux.

Afin d'assurer la validité et la fiabilité des résultats, nous avons utilisé la triangulation des sources, en comparant les informations issues de différents types de documents législatifs, académiques et professionnels, et en confrontant les perspectives de différents acteurs régulateurs, praticiens et chercheurs.

## 5. Cadre réglementaire et institutionnel du management des risques SI

### 5.1. Stratégie nationale de cybersécurité

Conscient des risques émergents de la cybersécurité, le Maroc a adopté la stratégie nationale de la cybersécurité dans le cadre de la stratégie de « Maroc Numeric 2013 » afin d'assurer la protection des systèmes d'informations des administrations, des organismes publics et des infrastructures d'importance vitale. Cette stratégie portait sur quatre axes principaux :

a) ***Évaluation des risques :*** Cet axe se concentre sur l'analyse des risques pesant sur les systèmes d'information pour identifier et estimer les pertes potentielles liées à des défaillances. L'objectif est de guider les efforts de sécurité à travers une approche dynamique et continue. Cet axe englobe deux programmes, le premier concerne l'élaboration des plans d'évaluation des risques et des menaces, et le deuxième consiste en la mise en place des outils d'aide à la décision.

b) ***Protection et défense des systèmes d'information :*** Cet axe aspire la mise en place des mesures de protection et de défense matérielle et immatérielle des systèmes d'information contre les différents types de menaces, et plus particulièrement les systèmes d'information des administrations, organismes publics et infrastructures d'importance vitale. Il inclut également la création de référentiels et normes nationaux de sécurité des technologies de l'information, le renforcement de la sécurité des systèmes informatiques et le renforcement des structures de veille, de détection, et de réponse aux incidents.

c) ***Renforcement des fondements de la sécurité :*** Ce pilier propose le développement d'un cadre juridique solide et adaptable constamment aux nouvelles mutations technologiques. Il consiste également sur l'élaboration des programmes de sensibilisation, de formation, ainsi que des initiatives de recherche et développement pour améliorer la sécurité des

ISSN: 2658-8455
Volume 5, Issue 10 (2024), pp. 317-346.

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

systèmes d'information. Il vise aussi à instaurer une culture de cybersécurité parmi tous les acteurs concernés.

d) ***Coopération nationale et internationale :*** Ce dernier axe souligne l'importance de la collaboration et du partage de connaissances et de ressources tant au niveau national qu'international pour combattre efficacement les cybermenaces.

Bien que la stratégie nationale de cybersécurité prévoyait une révision périodique pour tenir compte des nouvelles réalités et exigences (Hathaway & Spidalieri, 2018), il a fallu plus qu'une dizaine d'années afin qu'une nouvelle version soit publiée (fin du juillet 2024[3]) et qui porte sur quatre piliers principaux :

a) ***Gouvernance nationale de la cybersécurité et cadre institutionnel et juridique*** : Ce pilier se concentre sur la révision et le renforcement de cadre juridique et normatif qui régit la cybersécurité. Il ambitionne également à la promotion de la coordination entre les différents organes qui s'en chargent au contexte national.

b) ***Sécurité et résilience du cyberspace national*** : Ce pilier porte sur l'amélioration de la préparation nationale et la réactivité face aux menaces cybernétiques, la mise en place des indicateurs offrant une vision sur les capacités nationales en matière de cybersécurité, le renforcement des activités d'audit et de contrôle ainsi que la promotion de la mise en œuvre de standards nationaux de cybersécurité.

c) ***Développement des capacités et sensibilisation*** : La sensibilisation de la société est le cœur de ce pilier. Cette importance doit être accompagnée des mises à jour des programmes de formation, et la création de nouveaux cursus, renforçant ainsi les capacités des ressources humaines en matière de cybersécurité et encourageant l'innovation.

d) ***Coopération régionale et internationale*** : Ce pilier est le même que l'ancienne stratégie, insistant ainsi sur l'importance d'une collaboration nationale solide, et une coopération bilatérale accentuée avec les différents pays.

### 5.2. Lois et réglementations pertinentes

Au Maroc, à l'instar d'autres nations, les systèmes d'information jouent un rôle crucial dans le paysage économique. Dans un contexte marqué par la mondialisation et la digitalisation croissantes, le Maroc a entrepris de renforcer son infrastructure de systèmes d'information et de s'engager dans la course au numérique, aspirant à se positionner comme un leader sur le continent africain.

Nous allons essayer d'intégrer dans le tableau ci-dessous, seulement les textes législatifs et réglementaires qui sont les plus proches à la gestion des risques des systèmes d'information.

***Tableau 1: Cadre réglementaire de la gestion des risques des SI au Maroc***

| Objet | Points clés par rapport à la gestion des risques des SI |
|---|---|
| Loi n° 53-05 relative à l'échange électronique de données juridiques | La présente loi détermine le régime juridique applicable aux données juridiques échangées par voie électronique, notamment au moyen de techniques de cryptographie, ainsi qu'à la signature électronique (abrogée ensuite par la loi n°43-20). |
| Loi n° 43-20 relative aux services de confiance pour les transactions électroniques | La loi n° 43-20 relative aux services de confiance pour les transactions électroniques au Maroc met en place un cadre rigoureux pour la gestion des risques des systèmes d'information, en définissant les services de confiance, notamment les signatures électroniques et les cachets électroniques. Les prestataires de services de confiance doivent être agréés, et doivent utiliser des systèmes et |

[3] https://www.dgssi.gov.ma/fr/publications/strategie-nationale-de-cybersecurite *consulté le 27/08/2024*

ISSN: 2658-8455
Volume 5, Issue 10 (2024), pp. 317-346.

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

| Objet | Points clés par rapport à la gestion des risques des SI |
|---|---|
| | logiciels fiables, et assurer la sécurité technique et la fiabilité des processus. La loi impose des obligations strictes en matière de conservation et de protection des données, de notification des violations de sécurité, et de confidentialité des informations. La loi prévoit également des sanctions pour les manquements aux obligations légales, garantissant une dissuasion efficace contre les infractions. |
| Loi n° 05-20 relative à la cybersécurité | La loi 05-20 relative à la cybersécurité au Maroc impose des obligations aux administrations publiques, opérateurs de télécommunications, fournisseurs d'accès à Internet, prestataires de services numériques et toute autre personne morale de droit public de l'État, pour sécuriser leurs systèmes d'information. Elle exige l'élaboration de politiques de sécurité, la classification des informations sensibles, la désignation de responsables de sécurité, la mise en place de moyens de détection des incidents, et la notification immédiate des incidents à l'autorité nationale. La loi encadre strictement l'externalisation des systèmes d'information et impose des audits de sécurité réguliers. La loi prévoit également des sanctions sévères, renforçant ainsi la résilience des systèmes d'information contre les cybermenaces. |
| Loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel | Cette loi vise à garantir une protection robuste des données personnelles contre les abus et à harmoniser le cadre marocain de protection des données avec les normes internationales, notamment européennes. Elle établit également une Commission Nationale de Protection des Données Personnelles (CNDP) chargée de veiller à l'application de la loi.[4] |

***Source : Auteurs***

De même, le Maroc s'inscrit dans une démarche active de respect des différents règlements internationaux menaçant la sécurité des systèmes d'information, à savoir les conventions 108 et 108+ pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, le Règlement Général sur la Protection des Données (RGPD), et la convention Malabo de 2014 sur la cybersécurité et la protection des données à caractère personnel[5].

Il a aussi ratifié des conventions internationales telles que la Convention du Conseil de l'Europe sur la cybercriminalité et son protocole additionnel sur les infrastructures en nuage, et la Convention arabe contre les crimes liés aux technologies de l'information. Le gouvernement marocain ne publie pas de statistiques relatives à la cybercriminalité (Hathaway & Spidalieri, 2018). Le système juridique marocain poursuit plusieurs objectifs interconnectés, il vise à garder les libertés et les droits fondamentaux des citoyens dans l'ère numérique, à renforcer la confiance dans les échanges électroniques, à contrer efficacement les menaces cybernétiques ; et à cultiver un écosystème qui accueille chaleureusement l'évolution technologique. Néanmoins, les enjeux émergents liés à l'évolution rapide des technologies tels que

[4] https://www.dgssi.gov.ma/index.php/fr/loi-09-08-relative-la-protection-des-personnes-physiques-legard-du-traitement-des consulté le 21/06/2024
[5] https://www.cndp.ma/convention-malabo/ consulté le 22/06/2024

ISSN: 2658-8455
Volume 5, Issue 10 (2024), pp. 317-346.

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

l'intelligence artificielle, ne sont pas encore adaptés au contexte marocain, ou inclus dans son cadre réglementaire (Adnani & Haounani, 2024).

### 5.3. Institutions et organismes clés

Comme antérieurement mentionné, durant la stratégie nationale de « Maroc Digital 2013 », la stratégie nationale de cybersécurité a été adoptée, en fournissant la première feuille de route de gouvernance nationale pour la cybersécurité, axée sur le renforcement des capacités de sécurité, la sécurisation des infrastructures d'information critiques et la lutte contre la cybercriminalité. Plusieurs institutions et structures organisationnelles ont été créées pour soutenir ces objectifs.

a) ***Comité Stratégique de la Cybersécurité (CSC)*** : Ce comité a été créé par la loi n° 05-20 du 25 juillet 2020, en vue de piloter la mise en place des orientations stratégiques en matière de la cybersécurité au Maroc. De même, ce comité veille sur la résilience des systèmes d'information des administrations et des entités ayant des infrastructures d'importance vitale. Dirigé par le ministre délégué auprès du chef du gouvernement en charge de l'administration de la défense nationale, ce comité est composé des 14 divers ministres et administrations publiques, traduisant la volonté de Maroc à mettre la cybersécurité au cœur de ses préoccupations stratégiques.

b) ***Comité de gestion des crises et évènements cybernétiques majeurs*** : Ce comité a été créé également par la loi n°05-20 afin de garantir une intervention coordonnée en matière de prévention et de gestion de crise par suite d'incidents de cybersécurité. Il est présidé par la direction générale de la sécurité des systèmes d'information, et il est composé de huit représentants des autorités et organismes nationaux.

c) ***Direction Générale de la Sécurité des Systèmes d'Information*** : Désignée en tant que l'autorité nationale de la cybersécurité, la DGSSI a été créée par le décret n° 2-11-509 du 21 septembre 2011. Elle est rattachée à l'administration de la défense nationale du royaume du Maroc. Elle prend en charge le contrôle de la sécurité des systèmes d'information et adopte une approche solide pour garantir la résilience, la confidentialité, l'intégrité, et la disponibilité des données et des infrastructures.

d) ***Équipe marocaine d'intervention en cas d'urgence informatique (Moroccan Computer Emergency Response Team : ma-CERT)*** : Faisant partie de la DGSSI, cet organisme assure la mise en œuvre, en collaboration avec les autres administrations, de systèmes de veille, de détection et d'alerte des événements pouvant compromettre la sécurité des systèmes d'information de l'État, et coordonne la réponse à ces incidents au niveau national.

e) ***Commission Nationale de contrôle de la protection des Données à caractère Personnel (CNDP)*** : Créée par la loi n°09-08 du 18 février 2009, cette commission a pour mission de garantir le respect des libertés et droits fondamentaux des individus quant aux traitements de données à caractère personnel, et d'assurer la construction d'un écosystème célébrant la confiance numérique. Composée de six membres, et présidée par le directeur, tous nommés par sa majesté le roi Mohamed VI.

f) ***Laboratoire d'analyse de traces numériques*** : Relevant de la Brigade Nationale de la Police Judiciaire, procède à la recherche et à l'extraction de la preuve numérique incriminant les faits et informe les Officiers de Police Judiciaire, pour entamer la procédure, après accord du Parquet compétent (Abou El Jaouad 2023).

## 6. Normes et référentiels de gestion des risques SI

### 6.1. Référentiels nationaux développés par la DGSSI

La Direction Générale de la Sécurité des Systèmes d'Information est une entité créée par le décret n° 2-11-509 du 21 septembre 2011. Elle est rattachée à l'administration de la défense

ISSN: 2658-8455
Volume 5, Issue 10 (2024), pp. 317-346.

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

nationale du royaume du Maroc. Elle prend en charge le contrôle de la sécurité des systèmes d'information et adopte une approche solide pour garantir la résilience, la confidentialité, l'intégrité, et la disponibilité des données et des infrastructures critiques, tout en veillant à la conformité aux normes et réglementations nationales et internationales.

Les tableaux suivants synthétisent les référentiels, les guides, les directives, les outils ou les recommandations développées par la DGSSI. Les référentiels et les directives ont été mis dans un seul tableau (tableau 2). Les guides, les outils et les recommandations ont été groupés dans un deuxième tableau (tableau 3). La structure comportait pour chaque tableau ; le nom de document et son type, sa date de publication, sa compatibilité avec des standards ou des normes internationales, son champ d'application et ses objectifs principaux.

ISSN: 2658-8455
Volume 5, Issue 10 (2024), pp. 317-346.


IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

***Tableau 2: Référentiels et directives de la DGSSI***

| **Document** | **Date de publication** | **Compatibilité avec des standards internationaux** | **Champs d'application** | **Objectifs principaux** |
|---|---|---|---|---|
| Référentiel de gestion des incidents de cybersécurité | Première version en 2017<br>Dernière mise à jour en 2022 | ISO 27000<br>Publications spéciales NIST sur la gestion des incidents | Toutes les organisations | Assister dans la mise en place d'un système de gestion des incidents de cybersécurité, adéquat pour la garantie d'une proactivité maîtrisée face aux cyber incidents. |
| Référentiel de qualification des prestataires d'audit de la sécurité des Systèmes d'Information | Version initiale en 2018 et Dernière révision en 2024 | Norme ISO 19011 | Les prestataires d'audit | Qualifier les prestataires d'audit menés à contrôler les organismes disposant des systèmes d'information disponible, en regroupant les exigences relatives au prestataire d'audit, aux qualifications des auditeurs, et au déroulement de la prestation d'audit |
| Référentiel de vérification de la sécurité des applications | 2022 | La norme (ASVS) de l'OWASP, les normes de NIST, la norme PCI-DSS | Les organismes de développement | Assister les organismes à développer et à maintenir des applications sécurisées en respectant la confidentialité, l'intégrité et la disponibilité des informations traitées.<br>Faciliter l'alignement entre les besoins des parties prenantes et les offres de sécurité disponibles. |
| Directive nationale de la sécurité des systèmes d'information (DNSSI) | Publiée initialement en 2014 et mise à jour en 2023 | Aucune information n'était extraite | Les administrations de l'État, les établissements et entreprises publics, ainsi que toutes les Infrastructures d'Importance Vitale | Renforcer et harmoniser la sécurité des systèmes d'information de l'État et des infrastructures vitales |

***Source : Les données de ce tableau proviennent de la DGSSI 6***

[6] https://www.dgssi.gov.ma/fr/publications#documents consulté le 22/06/2024

ISSN: 2658-8455
Volume 5, Issue 10 (2024), pp. 317-346.


IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

***Tableau 3: Guides, recommandations et outils de la DGSSI***

| Document | Date de publication | Compatibilité avec des standards internationaux | Champs d'application | Objectifs principaux |
|---|---|---|---|---|
| Guide technique relatif à la sécurité du serveur Linux | 2014 | Aucune information n'était extraite | Responsables des entités disposant des serveurs Linux | Fournir des bonnes pratiques pour les administrateurs des systèmes Linux, en matière de la sécurité matérielle et logicielle |
| Guide de gestion des risques de la sécurité des systèmes d'information | 2014 | La famille ISO 27000 | Toutes les organisations | Survoler le processus de la gestion des risques en sécurité de l'information, et ses activités |
| Guide technique relatif à la sécurité des réseaux | 2014 | Normes de réseau tels que 802.1Q | Administrations et organismes publics | Proposer des recommandations et bonnes pratiques liées à la sécurité des réseaux |
| Guide régissant la sécurité relative à l'externalisation des SI | 2014 | Aucune information n'était extraite | Toutes les organisations | Assister dans la maîtrise de la sécurité des systèmes d'information externalisés |
| Guide de sécurité des applications Web | 2014 | Norme OWASP ASVS | Administrations et organismes publics | Supporter les responsables de la sécurité des systèmes d'information, pour la sécurisation de leurs applications web |
| Guide d'audit de la sécurité des systèmes d'information | 2015 | ISO 19011<br>La famille ISO 27000 | Administrations et organismes publics | Définir les besoins et les exigences en termes d'audit de la sécurité des systèmes d'information |
| Guide relatif à l'élaboration d'un plan de continuité et de reprise d'activités | 2016 | ISO 22301 | Entités et infrastructures d'importance vitale | Assister l'élaboration d'un plan de continuité d'activités à la suite d'un événement perturbant, et la diffusion des bonnes pratiques en matière de résilience. |
| Guide relatif à la sécurité des systèmes d'information industriels | 2017 | Aucune information n'était extraite | Entités avec des systèmes d'information industriels | Élever la sensibilisation aux vulnérabilités des systèmes d'information industriels<br>Mettre en œuvre une panoplie de mesures pour améliorer la cybersécurité des systèmes d'information industriels |
| Guide des bonnes pratiques-Évaluation de la maturité de la | 2021 | Normes de OSSA (Assurance de la sécurité des logiciels Oracle) | Développeurs de logiciels | Examiner le processus de développement logiciel dans son ensemble en fournissant des bonnes pratiques de la |

ISSN: 2658-8455
Volume 5, Issue 10 (2024), pp. 317-346.


| Document | Date de publication | Compatibilité avec des standards internationaux | Champs d'application | Objectifs principaux |
|---|---|---|---|---|
| sécurité du cycle de vie des développements logiciels | | | | sécurité logicielle tout au long de cycle de développement des logiciels |
| Guide d'homologation des systèmes d'information sensibles des infrastructures d'importance vitale | 2021 | Aucune information n'était extraite | Entités et infrastructures d'importance vitale | Assister les responsables des systèmes d'information sensibles dans l'homologation de la sécurité des systèmes avant la mise en exploitation. |
| Recommandations et bonnes pratiques de configuration des protocoles BGP et DNS | Aucune information n'était extraite | Normes de réseau tels que X.509 | Fournisseurs de service internet | Suggérer les bonnes pratiques en matière des protocoles d'échange sur les réseaux d'Internet |
| Outil d'évaluation de la conformité à la DNSSI | Aucune information n'était extraite | Aucune information n'était extraite | Entités et infrastructures d'importance vitale | Supporter les organismes souhaitant s'adapter à la DNSSI dans leur mise en conformité par rapport aux règles prescrites par la Directive. |

***Source : Les données de ce tableau proviennent de la DGSSI[7]***

.

[7] https://www.dgssi.gov.ma/index.php/fr/publications#guides consulté le 22/06/2024

ISSN: 2658-8455
Volume 5, Issue 10 (2024), pp. 317-346.

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

### 6.2. Normes adoptées par l'IMANOR

L'institut Marocain de normalisation (IMANOR), a été créé en 2014 par la loi n° 12-06 relative à la normalisation, la certification et l'accréditation. Il s'agit d'un établissement public, doté de la personnalité morale et de l'autonomie financière, placé sous la tutelle du ministère de l'Industrie, du Commerce, de l'Investissement et de l'Économie Numérique.
Le tableau suivant englobe la liste des normes liées à la gestion de système d'information, leur objet, leur nombre ainsi que leur date de publication. Les données sont issues du catalogue des normes IMANOR de 2023.

***Tableau 4: Référentiels et normes de l'IMANOR***

| Norme (sur la base d'indice de classement marocain) | Objet | Nombre des normes et dates de publication |
|---|---|---|
| Normes allant de 00.5.385 à 00.5.391 (correspondant à famille des normes ISO/IEC 38500) | Gouvernance des technologies de l'information | 5 normes : 2018 |
| Normes allant de 00.5.700 à 00.05.723 (correspondant à la famille des normes ISO/IEC 27000) | Systèmes de management de la sécurité de l'information | 18 normes : entre 2014 et 2022 |
| Normes allant de 00.5.742 à 00.5.752 (correspondant à la famille des normes ISO/IEC 20000) | Systèmes de management des services d'information | 10 normes : 2018 |
| Normes allant de 00.5.771 à 00.5.775 | Processus du cycle de vie de la délocalisation du processus d'affaires des services activés par IT | 5 normes : 2018 |
| Norme 17.0.001 | Technologies de l'information : Vocabulaires | 1 norme : 2015 |
| Normes allant de 17.0.060 à 17.0.071 | Mesures de sécurité d'archivage électronique des données | 12 normes : 11 normes en 2014 et la dernière en 2021 |
| Normes allant de 17.1.100 à 17.1.201 | Mesures d'accessibilité et d'adaptabilité | 8 normes : 2016 |
| Normes allant de 17.1.002 à 17.01.616 | Codage d'information | 101 normes : entre 2003 et 2016 |
| Normes allant de 17.1.621 à 17.1.623 | Mesures de la non-répudiation d'information | 3 normes : 2016 |
| Normes allant de 17.1.630 à 17.1.640 | Techniques de sécurité : cybersécurité | 7 normes : 2016 |
| Normes allant de 17.1.641 à 17.1.650 | Sécurité de réseau | 6 normes : 2016 |
| Normes allant de 17.1.652 à 17.3.034 | Génie logiciel et documentation des systèmes | 67 normes : entre 2013 et 2016 |
| Normes allant de 17.3.035 à 17.3.461 | Évaluation des processus et procédés informatiques | 23 normes : entre 2016 et 2021 |
| Normes allant de 17.3.462 à 17.3.469 | Procédures d'interconnexion des systèmes ouverts | 8 normes : 2018 |
| Normes allant de 17.4.001 jusqu'à 17.4.009 | Réseaux et interconnexion des systèmes ouverts | 9 normes : 2015 |
| Normes allant de 17.6.000 jusqu'à 17.6.105 | Systèmes à microprocesseurs terminaux et autres équipements périphériques matériel d'interface et d'interconnexion | 16 normes : entre 2015 et 2016 |
| Normes allant de 17.8.001 jusqu'à 17.8.467 | Application des technologies de l'information | 60 normes : entre 2007 et 2016 |
| Norme 17.9.001 | Mesures de sécurité du matériel de bureau | 1 norme : 2022 |

***Source : Catalogue IMANOR***[8]

[8] https://data.gov.ma/data/fr/dataset/catalogue-des-normes-marocaines-2023 *consulté le 25/06/2024*

ISSN: 2658-8455
Volume 5, Issue 10 (2024), pp. 317-346.

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

### 6.3. Comparaison avec les standards internationaux

Pour évaluer la pertinence et l'efficacité des normes et référentiels marocains en matière de gestion des risques SI, il est essentiel de les comparer aux standards internationaux reconnus. Cette comparaison permet d'identifier les forces, les faiblesses et les opportunités d'amélioration du cadre normatif marocain.

Tout d'abord, l'analyse des normes adoptées par l'IMANOR révèle un effort alignement avec la famille ISO 27000, en particulier la norme ISO/IEC 27001 pour les systèmes de management de la sécurité de l'information. On constate que les normes marocaines de la série 00.5.700 à 00.05.723 couvrent les aspects essentiels des systèmes de management de la sécurité de l'information, reflétant en grande partie les exigences de l'ISO 27001.

En outre, le référentiel de la DGSSI montre des similitudes avec le NIST Cybersecurity Framework, notamment dans l'approche basée sur les risques et la structure des domaines couverts. Toutefois, on peut noter que le cadre marocain semble mettre davantage l'accent sur la conformité réglementaire, reflétant les spécificités du contexte national, alors que le NIST Framework offre une flexibilité et une adaptabilité plus grandes, permettant aux organisations de différentes tailles et secteurs de l'appliquer plus facilement.

En comparaison avec les standards internationaux les plus récents, on constate que certains domaines émergents sont moins bien couverts dans les référentiels marocains. La gestion des risques liés à l'intelligence artificielle et au machine Learning, qui sont abordés dans les récentes mises à jour des standards internationaux, n'est pas encore prise en considération dans les référentiels marocains. Également, les aspects liés à la protection de la vie privée et à la conformité au règlement général sur la protection des données (RGPD) , bien que traités dans la loi 09-08, ne sont pas suffisamment intégrés dans les normes marocaines de gestion des risques SI.

D'autre part, un point fort des référentiels marocains est leur adaptation au contexte local. D'ailleurs, ils prennent en compte les spécificités du tissu économique marocain, notamment la prédominance des PME. Ils intègrent également des considérations liées au cadre juridique national, facilitant ainsi la conformité réglementaire des organisations marocaines.

Cependant, en comparaison avec les processus de révision réguliers des standards internationaux, le processus de mise à jour des normes et référentiels marocains semble moins structuré. Nous observons que les standards internationaux comme ISO 27001 ou le NIST Framework ont des cycles de révision bien définis, permettant une adaptation rapide aux nouvelles menaces et technologies. D'autre part, les référentiels marocains, bien que pertinents, ne semblent pas bénéficier d'un processus de révision aussi systématique, ce qui pourrait limiter leur capacité à suivre l'évolution rapide des risques SI.

En conclusion, bien que les normes et référentiels marocains montrent un alignement général avec les standards internationaux et une bonne adaptation au contexte local, il existe des opportunités d'amélioration, notamment en termes de couverture des domaines émergents et de processus de mise à jour. Une harmonisation plus étroite avec les standards internationaux, tout en maintenant l'adaptation aux spécificités locales, pourrait renforcer l'efficacité du cadre normatif marocain en matière de gestion des risques SI.

### 6.4. Applicabilité du processus de management des risques dans les cadres réglementaires et normatifs

Pour évaluer l'applicabilité du processus de management des risques des systèmes d'information dans le contexte marocain, il est essentiel d'examiner comment les différentes composantes de ce processus sont abordées dans les cadres réglementaires et normatifs existants. Cette analyse nous permet de comprendre dans quelle mesure ces cadres fournissent une base complète et

ISSN: 2658-8455
Volume 5, Issue 10 (2024), pp. 317-346.

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

cohérente pour la mise en œuvre effective des pratiques de gestion des risques SI dans les organisations marocaines.

Le tableau suivant présente une comparaison entre les éléments clés du processus de management des risques SI, tels qu'ils sont définis par les standards internationaux, et leur couverture dans les principaux textes législatifs et réglementaires marocains. Cette comparaison nous permettra d'identifier les forces et les lacunes potentielles du cadre marocain actuel.

ISSN: 2658-8455
Volume 5, Issue 10 (2024), pp. 317-346.


IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

***Tableau 5: Législation et réglementation vis à vis le processus de gestion des risques***

| Année | Textes législatifs /Réglementaires | Thématiques de gestion des risques des systèmes d'information | | | | | Commentaires |
|---|---|---|---|---|---|---|---|
| | | Établissement de contexte | Identification du risques | Analyse de risques | Évaluation de risques | Traitement des risques | |
| 1997 | Loi n° 24-96 consolidée relative à la poste et aux télécommunications | X | | | | | Dispositions contribuant à la sécurité et à la gestion des risques dans les télécommunications et les TIC |
| 2003 | Loi n° 07-03 complétant le code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données | X | | | | | Cadre juridique et pénal pour les infractions informatiques, encourageant la prévention et la protection |
| 2007 | Loi n° 53-05 relative à l'échange électronique de données juridiques | X | | | | X | Contribue au cadre général de gestion des risques SI, mais n'aborde pas les aspects opérationnels spécifiques |
| 2009 | Loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel | | X | | X | X | Gestion des risques axée sur la protection, la sécurité et la confidentialité des données personnelles |
| 2009 | Décret n° 2-09-165 du 25 Joumada i 1430 (21 mai 2009) pris pour l'application de la loi n° 09-08 | X | | | | | Établit des règles pour la sécurité et la confidentialité des données personnelles, assurant la conformité réglementaire |
| 2009 | Décret n° 2-08-518 du 21 mai 2009 pris pour l'application des articles 13, 14, 15, 21 et 23 de la loi n° 53-05 | X | | | | | Spécifie des mesures techniques et organisationnelles pour sécuriser les échanges électroniques de données juridiques |
| 2011 | Loi n° 31-08 édictant des mesures de protection du consommateur, y compris la protection du consommateur en ligne | X | | | | | Renforce indirectement la sécurité des transactions en ligne, sans focus spécifique sur la gestion des risques SI |
| 2011 | Décret n°2-11-509 du 22 chaoual 1432 (21 septembre 2011) complétant le décret n° 2-82-673 du 28 rabii i 1403 (13 janvier 1983) relatif à | X | | | | | Importance dans la sécurité nationale et la protection des systèmes d'information stratégiques |

ISSN: 2658-8455
Volume 5, Issue 10 (2024), pp. 317-346.


| Année | Textes législatifs /Réglementaires | Thématiques de gestion des risques des systèmes d'information | | | | | Commentaires |
|---|---|---|---|---|---|---|---|
| | | Établissement de contexte | Identification du risques | Analyse de risques | Évaluation de risques | Traitement des risques | |
| | l'organisation de l'ADN et portant création de la DGSSI | | | | | | |
| 2015 | Décret n° 2-13-881 du 20 janvier 2015 modifiant et complétant le décret n° 2-08-518 du 25 Joumada i 1430 (21 mai 2009) | X | | | X | | Définit des normes de sécurité, des obligations et des procédures pour la gestion des risques SI |
| 2020 | Loi n° 43-20 relative aux services de confiance pour les transactions électroniques | X | | | | | Implications indirectes sur la gestion des risques SI via des exigences de sécurité spécifiques, sans aborder explicitement le processus de gestion |
| 2020 | Loi n° 05-20 relative à la cybersécurité | X | | X | X | | Établit un cadre général de gestion des risques SI, sans entrer dans les détails opérationnels du processus |
| 2021 | Décret n° 2-21-406 du 15 juillet 2021 pris pour l'application de la loi n° 05-20 relative à la cybersécurité | | | | | X | Établit un cadre réglementaire pour la cybersécurité, incluant des mesures préventives et réactives. |
| 2022 | Décret n° 2-22-687 du 16 novembre 2022 pris pour l'application de la loi n°43-20 | X | | | | | Encourage l'établissement de normes de sécurité et de mécanismes de certification pour les services de confiance électronique. |

***Source : Auteurs***

ISSN: 2658-8455
Volume 5, Issue 10 (2024), pp. 317-346.

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

L'examen détaillé des textes réglementaires révèle des variations significatives dans le traitement du processus de management des risques des systèmes d'information (SI). Un point commun à la majorité des documents est l'accentuation sur l'établissement du contexte, reflétant une approche qui privilégie la compréhension de l'environnement organisationnel et réglementaire.
Cependant, des lacunes subsistent, notamment dans le traitement spécifique des risques. Alors que l'identification et l'évaluation des risques sont généralement bien couvertes, les détails concernant la mise en œuvre de stratégies de gestion adaptées au cadre réglementaire et normatif marocain restent incomplets. Cette insuffisance de précision peut entraver l'efficacité du processus de management des risques SI.
De plus, bien que les textes législatifs et réglementaires couvrent globalement les principales étapes du processus de gestion des risques, l'absence de directives claires pour la mise en œuvre de mesures concrètes peut laisser les organisations dans une incertitude opérationnelle. Cette couverture variée selon les secteurs est particulièrement évidente lorsqu'on compare la loi n° 05-20 relative à la cybersécurité, qui propose une approche plus intégrée, à d'autres textes qui se focalisent sur des aspects spécifiques, reflétant potentiellement des priorités sectorielles.
En conclusion, il existe des opportunités significatives pour renforcer l'applicabilité du processus de management des risques SI. L'élaboration de directives plus détaillées pour l'analyse et le traitement des risques, le développement des guides pratiques ou des normes complémentaires ainsi que la recherche d'une plus grande harmonisation entre les différents cadres réglementaires, sont des étapes clés pour renforcer la gestion des risques dans le contexte marocain. Ces améliorations contribueront à une meilleure préparation et résilience des organisations face aux risques associés aux systèmes d'information.

## 7. Analyse de l'applicabilité et de l'adoption de cadres réglementaires et normatifs par les organisations

### 7.1. État des lieux des pratiques dans les grandes entreprises

L'adoption et la mise en œuvre du management des risques SI dans les grandes entreprises marocaines présentent un tableau contrasté. Selon l'étude réalisée en 2024 par PwC en collaboration avec l'Association Des Utilisateurs Des Systèmes D'Information Au Maroc (AUSIM), 96% des entreprises interrogées plébiscitent le cadre ISO 27001 pour évaluer leur posture de cybersécurité. Cependant, les statistiques de la certification partagées par l'Organisme International de la Standardisation (ISO) présentent des constats divergents.
En 2021 et 2022, seulement 40 entreprises au Maroc étaient certifiées ISO 27001:2017. La répartition sectorielle de ces certifications est révélatrice ; 28 dans le secteur des technologies de l'information, 2 dans le transport, entreposage & communication, 1 dans le commerce de gros et de détail, 1 dans l'intermédiation financière et l'immobilier et 8 dans des secteurs non spécifiés. Ces chiffres suggèrent un écart significatif entre l'intention d'adopter des pratiques de gestion des risques SI conformes aux standards internationaux et leur mise en œuvre effective.
Les grandes entreprises, en particulier dans les secteurs réglementés comme la finance et les télécommunications (Maroc Telecom[9], Orange[10] et INWI[11]), montrent une plus grande maturité dans l'adoption de pratiques formelles de gestion des risques SI. Cette disparité peut s'expliquer

[9] https://www.iam.ma/groupe-maroc-telecom/responsabilite-societale-dev-durable/certifications-labels/certification-securite-de-l-Information-iso-271001.aspx consulté le 27/08/2024
[10] https://cloud.orange-business.com/certifications/certifications-des-offres-de-cloud/certification-iso-27001/ consulté le 27/08/2024
[11] https://fr.le360.ma/economie/inwi-decroche-la-certification-iso-27001-pour-son-datacenter-a-rabat-technopolis-210365/ consulté le 27/08/2024

ISSN: 2658-8455
Volume 5, Issue 10 (2024), pp. 317-346.

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

par plusieurs facteurs intrinsèques aux grandes entreprises. Tout d'abord, ces organisations disposent généralement de ressources financières et humaines plus importantes, leur permettant d'investir davantage dans des systèmes de sécurité robustes et d'embaucher des experts en cybersécurité. De plus, leur taille et leur visibilité accrues les exposent davantage aux risques cybernétiques, les incitant à renforcer leurs défenses. Enfin, ces entreprises sont souvent soumises à des exigences réglementaires plus strictes, les obligeant à mettre en place des mesures de sécurité plus avancées pour se conformer aux normes en vigueur.
Toutefois, même parmi ces grandes entreprises, Boulafdour & Kounaidi (2018) ont observé l'absence fréquente de processus formalisés de gestion des risques, ce qui peut entraver l'identification, l'évaluation, le traitement et la communication efficaces des risques.

### 7.2. Défis spécifiques aux PME

Les PME, qui constituent l'épine dorsale de l'économie marocaine, font face à des défis particuliers dans l'adoption et la mise en œuvre du management des risques SI. M. Chouki et al. (2018) soulignent que les PME marocaines sont souvent confrontées à des contraintes de taille et de ressources qui limitent leur capacité à investir dans des systèmes et des pratiques de gestion des risques SI sophistiqués. Cette limitation en ressources se reflète dans les observations de Matrane & Talea (2014) qui ont constaté que les PME marocaines se concentrent principalement sur la définition des objectifs de gestion des risques et l'évaluation du niveau de risque global, mais peinent à mettre en place des pratiques plus avancées. Oufkir & Ouhadi (2024) ont mis en évidence une autre dimension du problème en identifiant une résistance au changement chez certains dirigeants de PME, liée à une réticence à assumer des risques de croissance et à une attitude fataliste ancrée dans la culture locale. Par ailleurs, Raissouni et al. (2023) ont identifié le manque de personnel qualifié comme l'un des obstacles majeurs à la mise en œuvre de mesures de sécurité efficaces dans les entreprises marocaines. Ces mêmes auteurs soulignent également que les coûts élevés d'acquisition et de mise en œuvre des technologies de sécurité, ainsi que les dépenses liées à la formation et à la sensibilisation, sont souvent perçus comme des freins importants par les PME. Ces différents facteurs combinés expliquent en grande partie les difficultés rencontrées par les PME marocaines dans le domaine du management des risques SI.

### 7.3. Analyse des écarts entre le cadre réglementaire et la pratique

Malgré un cadre réglementaire et normatif relativement développé, on constate un écart significatif entre les exigences légales et les pratiques effectives des organisations marocaines en matière de gestion des risques SI. Ce décalage se manifeste de plusieurs manières au sein des entreprises marocaines.
Tout d'abord, on observe une tendance à la conformité sélective. Les organisations tendent à se conformer aux aspects les plus visibles ou les plus strictement contrôlés de la réglementation, négligeant parfois des aspects qu'elles considèrent plus subtils mais tout aussi importants de la gestion des risques SI. Cette approche partielle compromet l'efficacité globale des mesures de sécurité mises en place.
Par ailleurs, Kerraous (2018) a observé que de nombreuses entreprises adoptent une approche réactive plutôt que proactive dans la gestion des risques SI, réagissant aux incidents plutôt que de les anticiper. Cette attitude résulte en des interruptions opérationnelles et des coûts relativement élevés de correction, qui pourraient être maîtrisés avec des outils de prévention adéquats.
Le manque d'intégration des mesures de sécurité dans une stratégie globale de gestion des risques SI est un autre problème souligné par (Boulafdour & Kounaidi, 2018). Même lorsque des mesures de sécurité sont mises en place, elles ne sont pas toujours intégrées dans une

ISSN: 2658-8455
Volume 5, Issue 10 (2024), pp. 317-346.

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

approche cohérente et globale. Ce manque d'intégration peut entraîner une vulnérabilité accrue aux cyberattaques, une non-conformité aux régulations, et une inefficacité opérationnelle.
On constate également des disparités sectorielles importantes. L'adoption et la mise en œuvre des pratiques de gestion des risques SI varient considérablement selon les secteurs, avec une plus grande maturité dans les secteurs réglementés comme la finance et les télécommunications. En revanche, ces pratiques sont très faibles, voire absentes, dans d'autres secteurs de service tels que le transport, limitant ainsi l'efficacité, l'innovation et la compétitivité globale de ces secteurs.
Enfin, il existe une tendance à se focaliser sur la conformité réglementaire plutôt que sur l'efficacité réelle des mesures de gestion des risques SI. Cette approche peut conduire à une application superficielle des pratiques, mettant en danger la sécurité des actifs informationnels. Les organisations risquent ainsi de se conformer aux exigences réglementaires sans pour autant mettre en place des mesures véritablement efficaces pour protéger leurs systèmes d'information.
En conclusion, bien que le Maroc ait fait des progrès significatifs dans l'établissement d'un cadre réglementaire et normatif pour la gestion des risques SI, l'adoption et la mise en œuvre effectives de ces pratiques restent un défi, en particulier pour les PME. Les facteurs culturels, organisationnels et économiques jouent un rôle crucial dans cet écart entre la théorie et la pratique, soulignant la nécessité d'une approche plus adaptée et contextualisée pour améliorer la maturité du management des risques SI dans les organisations.

## 8. Facteurs culturels et organisationnels influençant le management des risques SI

### 8.1. Impact de la culture organisationnelle

La culture organisationnelle joue un rôle crucial dans l'adoption et l'efficacité des pratiques de management des risques SI au Maroc. Plusieurs aspects de cette culture ont été identifiés comme exerçant une influence significative sur la gestion des risques liés aux systèmes d'information.
La structure hiérarchique traditionnelle dans de nombreuses organisations marocaines peut influencer la manière dont les risques sont perçus et gérés. M. Chouki et al. (2018) ont souligné que la prise de décision centralisée peut parfois entraver une approche proactive et collaborative de la gestion des risques SI. Cette centralisation peut limiter la capacité de l'organisation à réagir rapidement aux menaces émergentes et à impliquer tous les niveaux de l'entreprise dans la stratégie de sécurité.
Les problèmes de communication interne, également identifiés comme un défi par (M. Chouki et al., 2018), peuvent affecter la diffusion efficace des politiques de sécurité et la sensibilisation aux risques SI à tous les niveaux de l'organisation. Une communication déficiente peut entraîner une méconnaissance des risques et des procédures de sécurité, augmentant ainsi la vulnérabilité de l'entreprise aux menaces informatiques.
L'attitude envers le changement est un autre facteur culturel important. La résistance au changement, observée par (Oufkir & Ouhadi, 2024), particulièrement dans les PME, peut freiner l'adoption de nouvelles pratiques de gestion des risques SI, même lorsque leur nécessité est reconnue. Cette résistance peut se manifester par une réticence à modifier les habitudes de travail ou à investir dans de nouvelles technologies de sécurité.
La valorisation de la sécurité au sein de la culture d'entreprise est un aspect crucial souligné par (Chang & Ho, 2006). Au Maroc, le degré de priorité accordé à la sécurité des SI varie considérablement selon les organisations et les secteurs. On observe une forte valorisation dans des secteurs vitaux tels que la finance et les télécommunications, où les enjeux de sécurité sont particulièrement critiques. En revanche, cette valorisation devient faible, voire absente, dans

ISSN: 2658-8455
Volume 5, Issue 10 (2024), pp. 317-346.

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

d'autres secteurs, ce qui peut conduire à une sous-estimation des risques et à une vulnérabilité accrue.
Ces différents aspects de la culture organisationnelle interagissent et influencent collectivement la capacité des entreprises marocaines à mettre en place et à maintenir des pratiques efficaces de gestion des risques SI.

### 8.2. Attitudes culturelles vis-à-vis du risque et de l'incertitude

Les attitudes culturelles marocaines envers le risque et l'incertitude ont un impact significatif sur la manière dont les organisations abordent le management des risques SI. Ces attitudes se manifestent de diverses manières et influencent les pratiques de gestion des risques au sein des entreprises marocaines.
Oufkir & Ouhadi (2024) ont observé une tendance au fatalisme chez certains dirigeants de PME marocaines, qui perçoivent les risques comme inévitables ou hors de leur contrôle. Cette attitude fataliste peut conduire à une approche passive de la gestion des risques SI, où les menaces sont considérées comme des événements inéluctables plutôt que des défis à anticiper et à gérer activement. Cette perspective peut freiner la mise en place de mesures préventives efficaces et limiter la résilience des organisations face aux cybermenaces.
Par ailleurs, Kadmiri et al. (2021) ont souligné la nécessité d'adapter les stratégies de gestion des risques au contexte local. Ils ont notamment mis en évidence une tension entre la perception à court terme et à long terme des risques. La tendance à privilégier les résultats à court terme, souvent observée dans le contexte marocain, peut parfois entrer en conflit avec la nature à long terme des investissements en sécurité des SI.
Un autre aspect culturel important est la prédominance de la confiance interpersonnelle sur la confiance dans les systèmes formels. La confiance en tant qu'une valeur ancrée dans la culture marocaine est souvent basée sur les relations personnelles (Soufiane, 2020) plutôt que sur des procédures ou des systèmes institutionnels. Cette caractéristique peut influencer la manière dont les politiques de sécurité sont perçues et mises en œuvre. Les employés peuvent être plus enclins à suivre des directives de sécurité émanant de personnes en qui ils ont confiance plutôt que de se conformer strictement à des politiques formelles, ce qui peut créer des défis dans l'application uniforme des mesures de sécurité.
En outre, l'attitude envers l'incertitude joue un rôle crucial dans la gestion des risques SI. Akhlaffou (2020) a observé dans la culture marocaine un faible contrôle de l'incertitude, attribué en partie au concept de "Maktoub" (ce qui est écrit, ou prédestiné). Cette notion culturelle tend à atténuer l'anxiété des individus face aux événements imprévisibles, impactant ainsi leur approche de la gestion des risques. Dans le contexte des systèmes d'information, cette attitude peut avoir des implications significatives sur la volonté des organisations à investir dans des mesures de prévention. Paradoxalement, bien que la culture générale montre une plus grande tolérance à l'incertitude, les réactions organisationnelles peuvent varier. Certaines entreprises, conscientes de cette tendance culturelle, pourraient adopter une approche plus proactive et instaurer des mesures de sécurité robustes pour contrebalancer cette attitude. D'autres pourraient, au contraire, se conformer à cette tolérance culturelle à l'incertitude, adoptant une approche plus flexible mais potentiellement moins systématique dans leur gestion des risques SI. Cette diversité d'approches souligne la complexité de l'interaction entre les facteurs culturels et les pratiques organisationnelles dans le domaine de la sécurité de l'information au Maroc.

### 8.3. Enjeux de formation et de sensibilisation

La formation et la sensibilisation jouent un rôle crucial dans l'établissement d'une culture de sécurité efficace au sein des organisations marocaines. Plusieurs études ont mis en lumière l'importance de ces aspects dans le contexte de la gestion des risques des systèmes d'information.

ISSN: 2658-8455
Volume 5, Issue 10 (2024), pp. 317-346.

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

Raissouni et al. (2023) ont identifié le manque de personnel qualifié comme un obstacle majeur à la mise en œuvre de mesures de sécurité efficaces. Cette constatation souligne l'importance cruciale de la formation et de la sensibilisation dans le développement des compétences nécessaires à une gestion efficace des risques SI. Dans cette optique, Kerraous (2018) a observé que la majorité des entreprises interrogées dans son étude organisent des formations à la gestion des risques. Cette pratique témoigne d'une reconnaissance croissante du rôle de la formation dans l'amélioration de la culture du risque au sein des organisations marocaines.

Cependant, l'efficacité de ces programmes de sensibilisation varie considérablement selon les organisations. Siponen (2000) a souligné l'importance d'une approche méthodique et structurée dans l'élaboration de programmes de sensibilisation à la sécurité de l'information. Dans le contexte marocain, Moussir & Liouaeddine (2021) ont noté que la proportion des entreprises offrant une formation continue à leurs employés reste faible, avec une prédominance dans le secteur des services.

La continuité de la formation représente un autre défi important. Yaraghi & Langhe (2011) ont insisté sur le rôle crucial de la formation continue pour une gestion efficace des risques SI. Néanmoins, dans le contexte marocain, la régularité et la mise à jour de ces formations restent un défi pour de nombreuses organisations.

Ces observations mettent en évidence la nécessité d'une approche plus systématique et continue de la formation et de la sensibilisation en matière de gestion des risques SI au Maroc. Bien que des progrès aient été réalisés, il reste encore des efforts à fournir pour assurer une diffusion large et efficace des connaissances et des compétences nécessaires à une gestion des risques SI robuste et adaptée au contexte local.

### 8.4. Influence des facteurs économiques et structurels

La structure économique du Maroc, caractérisée par une prédominance PME, influence significativement la gestion des risques des systèmes d'information (SI). Abaaoukide & Bentaleb (2011) ont mis en lumière le rôle central des PME dans l'économie marocaine, soulignant que ces entités rencontrent des défis particuliers liés à la limitation des ressources et à l'expertise nécessaire pour une gestion efficace des risques SI. Ces contraintes se manifestent notamment dans la difficulté à mobiliser les investissements requis pour la sécurité des SI, exacerbée par des contraintes budgétaires substantielles. (Raissouni et al., 2023) ont identifié le coût élevé de l'acquisition et de la mise en œuvre des technologies de sécurité comme un frein important pour de nombreuses organisations marocaines.

En outre, la pression concurrentielle intense sur le marché peut parfois inciter les entreprises à déprioriser les investissements dans la sécurité des SI, perçus comme non directement productifs dans un environnement économique en rapide évolution. Cette focalisation sur le développement commercial en négligeant la sécurité des infrastructures informationnelles peut mettre en péril l'intégrité et la sécurité de l'information.

En conclusion, les facteurs culturels et organisationnels jouent un rôle déterminant dans la manière dont les organisations marocaines abordent le management des risques SI. La prise en compte de ces facteurs est essentielle pour développer des approches efficaces et adaptées au contexte local. Cette initiative implique non seulement des efforts en matière de formation et de sensibilisation, mais aussi une adaptation des méthodes et outils de gestion des risques SI aux spécificités culturelles et organisationnelles marocaines.

## 9. Discussion

La présente analyse de l'état des lieux du management des risques SI au Maroc révèle un paysage évolutif et complexe. Bien que le Maroc ait mis en place un cadre réglementaire et normatif relativement avancé, son applicabilité et efficacité varient selon les secteurs et la taille

ISSN: 2658-8455
Volume 5, Issue 10 (2024), pp. 317-346.

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

des organisations. Cet écart est particulièrement prononcé dans les PME, qui constituent la majorité du tissu économique marocain.

Cette variabilité peut être expliquée par la théorie de la contingence, qui soutient que l'efficacité des stratégies organisationnelles dépend des caractéristiques spécifiques de leur environnement. Ainsi, dans des secteurs fortement régulés comme les télécommunications, les entreprises marocaines tendent à mieux appliquer les normes de cybersécurité, sous la pression des régulateurs et en raison des risques élevés associés à leurs activités. En revanche, dans des secteurs moins régulés ou chez les petites et moyennes entreprises, la gestion des risques SI peut être moins priorisée, les ressources étant souvent limitées et les pressions institutionnelles moins fortes. Cette approche contingente montre que, malgré un cadre normatif avancé, l'efficacité des pratiques de gestion des risques dépend largement des contextes spécifiques des entreprises au Maroc.

L'influence des facteurs culturels s'avère cruciale dans l'adoption et l'efficacité des pratiques de gestion des risques SI. Les attitudes culturelles envers le risque, la hiérarchie organisationnelle et la résistance au changement jouent un rôle déterminant dans la mise en œuvre de ces pratiques. Par ailleurs, les PME marocaines font face à des défis particuliers, notamment en termes de ressources, d'expertise et de sensibilisation aux risques SI. Dans ce contexte, la formation et la sensibilisation émergent comme des facteurs clés pour améliorer la culture de sécurité et l'efficacité du management des risques SI.

Ces constats ont des implications importantes pour la théorie et la pratique du management des risques SI dans le contexte marocain. Les modèles théoriques de gestion des risques SI doivent être aux spécificités culturelles et organisationnelles marocaines, favorisant une approche plus contextuelle.

En outre, des efforts sont nécessaires pour réduire l'écart entre les exigences réglementaires et les pratiques organisationnelles, notamment par le biais de guides pratiques et de mécanismes de soutien. Les stratégies de sécurité des SI doivent intégrer explicitement les facteurs culturels pour être efficaces dans le contexte marocain. De plus, une approche différenciée par secteur pourrait être plus efficace, reconnaissant les différences de maturité et de besoins entre les différents secteurs de l'économie marocaine.

Sur la base de ces constats et implications, plusieurs recommandations peuvent être formulées pour améliorer la maturité du management des risques SI au Maroc. Il est crucial de renforcer les programmes de formation existants et d'en développer de nouveaux, adaptés aux différents niveaux organisationnels et secteurs. L'accent doit être mis également sur la création d'une culture qui fait de la sécurité des systèmes d'information une priorité stratégique. L'instauration de politiques de sensibilisation au sein des organisations, déployant divers moyens tels que des capsules vidéo, des réunions, des séminaires et des courriels personnalisés, peut contribuer à renforcer la résilience organisationnelle contre les menaces.

Pour les PME, il est essentiel de mettre en place des mécanismes de soutien spécifiques, tels que des guides simplifiés, des outils d'auto-évaluation et des incitations financières pour l'adoption de pratiques de gestion des risques SI. La collaboration entre les organismes gouvernementaux et le secteur privé doit être renforcée pour partager les meilleures pratiques et les informations sur les menaces, favorisant une participation active de tous les acteurs.

Le développement de normes et de référentiels locaux, alignés sur les standards internationaux et prenant en compte les évolutions technologiques et les spécificités du contexte marocain, est également recommandé. Cela permettrait de renforcer la sécurité et la compétitivité des entreprises marocaines sur le plan international.

De surcroît, l'intégration de la gestion des risques SI dans les processus plus larges de gouvernance d'entreprise et de gestion des risques est cruciale pour assurer une compréhension approfondie des enjeux de la sécurité de l'information. Par ailleurs, la stimulation de la recherche académique et appliquée sur le management des risques SI dans le contexte marocain

ISSN: 2658-8455
Volume 5, Issue 10 (2024), pp. 317-346.

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

contribuerait à développer des connaissances et des solutions adaptées, enrichissant ainsi le paysage académique national et améliorant ces pratiques au sein des organisations.
L'amélioration des processus de contrôle et d'audit est essentielle pour assurer une meilleure conformité aux exigences réglementaires et aux bonnes pratiques de gestion des risques SI. De plus, l'investissement dans le développement de compétences locales en cybersécurité, notamment par le biais de partenariats entre universités et entreprises, est crucial. Ces éléments sont fondamentaux pour renforcer la capacité du pays à répondre efficacement aux cybermenaces.
En conclusion, l'amélioration de la maturité du management des risques SI au Maroc nécessite une approche holistique qui prenne en compte les aspects réglementaires, culturels, organisationnels et économiques. Cette approche doit être flexible et adaptative pour répondre aux besoins spécifiques des différentes organisations et secteurs, tout en s'alignant sur les meilleures pratiques internationales. Le succès de cette démarche repose sur un engagement continu de toutes les parties prenantes, des décideurs politiques aux employés individuels, dans la création d'une culture de sécurité robuste et adaptée au contexte marocain.

## 10. Conclusion et perspectives futures

Cette étude a dressé un état des lieux détaillé du management des risques des systèmes d'information au Maroc, mettant en lumière plusieurs aspects clés. Elle a révélé que malgré l'établissement d'un cadre réglementaire ambitieux et aligné sur les standards internationaux, il existe un écart significatif entre les exigences réglementaires et les pratiques effectives des organisations, particulièrement au sein des PME. Ceci peut être justifié par le fait que les entreprises ne sont pas assez conscientes et ne se trouvent pas dans l'obligation d'adhérer à ces cadres, malgré leur vitalité. L'analyse a également souligné l'impact crucial des facteurs culturels et organisationnels sur l'adoption et l'efficacité des pratiques de gestion des risques SI, ainsi que les défis particuliers auxquels font face les PME marocaines dans ce domaine. De plus, la recherche a mis en évidence le rôle central de la formation et de la sensibilisation dans l'amélioration de la maturité du management des risques SI.
Malgré une approche méthodologique rigoureuse, cette étude présente certaines limites qu'il convient de reconnaître. Il est important de noter que la présente analyse, basée sur une revue documentaire approfondie, constitue la première phase de la recherche et sera complétée ultérieurement par une étude empirique impliquant des enquêtes et des entretiens directs avec des experts du domaine. Cette phase pratique, qui traitera directement avec les professionnels sur le terrain, fera l'objet d'une publication séparée au moment opportun. Par la même occasion, nous notons la disponibilité limitée de données quantitatives sur l'adoption des pratiques de gestion des risques SI qui restreint la possibilité de généraliser certains résultats, et d'approfondir des analyses comparatives entre le contexte marocain et d'autres contextes internationaux.
De plus, la nature dynamique du domaine de la cybersécurité implique que certaines informations, notamment concernant les cadres réglementaires, peuvent évoluer rapidement. Néanmoins, la méthodologie adoptée a permis de fournir une vue d'ensemble substantielle et critique de l'état actuel du management des risques SI au Maroc, offrant ainsi une base solide pour la discussion et l'élaboration de recommandations.
Cette étude ouvre plusieurs pistes pour de futures recherches. Des études de cas approfondies sur des organisations marocaines de différentes tailles et secteurs pourraient fournir des perspectives plus précises sur les pratiques de gestion des risques SI. Une étude quantitative à grande échelle permettrait de mesurer plus précisément le niveau d'adoption et d'efficacité de ces pratiques au Maroc. Une comparaison avec d'autres pays émergents aiderait à identifier les meilleures pratiques et les défis communs dans des contextes similaires. D'autres pistes incluent

ISSN: 2658-8455
Volume 5, Issue 10 (2024), pp. 317-346.

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

l'évaluation de l'impact des programmes de formation, l'étude des facteurs de résilience des organisations marocaines face aux cybermenaces, et l'analyse de l'impact économique des incidents de cybersécurité et des investissements en gestion des risques SI au Maroc.

En conclusion, cette étude a fourni une base solide pour comprendre l'état actuel du management des risques SI au Maroc. Elle souligne la nécessité d'une approche holistique et contextualisée, prenant en compte les spécificités culturelles, organisationnelles et économiques du pays. Les futures recherches dans ce domaine seront cruciales pour accompagner l'évolution du paysage numérique marocain et renforcer la résilience des organisations face aux défis croissants de la cybersécurité. L'amélioration continue de la maturité du management des risques SI au Maroc nécessitera un effort soutenu et collaboratif de toutes les parties prenantes, des décideurs politiques aux praticiens sur le terrain.

**Références**

(1). Abaaoukide, K., & Bentaleb, C. (2011). La gestion de l'urgence dans les PME au Maroc : Perceptions et pratiques de gestion. *Revue Management et Avenir*, *3*, 143-163.

(2). ADNANI, E., & HAOUNANI, A. (2024). L'Intelligence Artificielle au Maroc : Entre éthique et réglementation. *Revue Internationale de la Recherche Scientifique (Revue-IRS)*, *2*(3), 1234-1252.

(3). Akhlaffou, M. (2020). Culture nationale et pratiques managériales au sein des organisations marocaines : Une enquête empirique. *Revue Economie, Gestion et Société*, *1*(22).

(4). Amien, I. (2014). *Learning from risk : Facilitating organizational learning through enterprise risk management* [Thesis, Stellenbosch University]. http://hdl.handle.net/10019.1/86517

(5). Argyris, Ch. (1977). Double loop learning in organizations. *Harvard Business Review*, *55*(5), 115-125.

(6). Argyris, Ch., & Schön, D. A. (1997). Organizational Learning : A Theory of Action Perspective. *Reis*, *77/78*, 345-348. JSTOR. https://doi.org/10.2307/40183951

(7). 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.

(8). Bighrissen, B., & Cherkaoui, C. (2012). Towards the success of ERP systems : Case study in two Moroccan companies. *Journal of Enterprise Resource Planning Studies*, 1.

(9). BOULAFDOUR, B., & KOUNAIDI, M. (2018). La gouvernance des systèmes d'information au Maroc : Une étude empirique. *Revue du Contrôle, de la Comptabilité et de l'Audit*, *2*(3).

(10). Braes, B., & Brooks, D. (2011). Organizational Resilience : Understanding and identifying the essential concepts. *Safety and Security Engineering IV*, *117*, 117-128.

(11). Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, *3*(2), 77-101.

(12). Chang, S. E., & Ho, C. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management and Data Systems*, *106*, 345-361. https://doi.org/10.1108/02635570610653498

(13). Chergui, M., Nahla, H., Chakir, A., Elhassnaoui, S., Sekhara, Y., & Medromi, H. (2016). Empirical study : Moroccan information systems specificities for better IT governance. *International Journal of Advanced Engineering, Management and Science*, *2*(5), 391-396.

ISSN: 2658-8455
Volume 5, Issue 10 (2024), pp. 317-346.

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

(14). Chowdhury, D. (2004). Incentives, control, and development : Governance in private and public sector with special reference to Bangladesh. *(No Title)*.
(15). Dekker, S. W. (2013). Drifting into failure : Complexity theory and the management of risk. In *Chaos and complexity theory for management : Nonlinear dynamics* (p. 241-253). IGI Global.
(16). Desender, K. (2011). On the determinants of enterprise risk management implementation. In *Enterprise IT governance, business value and performance measurement* (p. 87-100). IGI Global.
(17). El Abbassi, A., & Chafik, K. (2014). The Decision to Invest in Information Systems : Case of Adopting ERP in the Moroccan Public Largest Companies. *International Journal of Computer Applications*, *88*(15).
(18). Emblemsvåg, J. (2020). Risk and complexity–on complex risk management. *The Journal of Risk Finance*, *21*(1), 37-54. https://doi.org/10.1108/JRF-09-2019-0165
(19). Freeman, R. E. (2010). *Stakeholder Theory : The State of the Art*. Cambridge University Press.
(20). Hathaway, M., & Spidalieri, F. (2018). KINGDOM OF MOROCCO:CYBER READINESS AT A GLANCE. *Potomacinstitute*.
(21). Jackson, S. (2011). Organizational culture and information systems adoption : A three-perspective approach. *Information and Organization*, *21*(2), 57-83. https://doi.org/10.1016/j.infoandorg.2011.03.003
(22). Kadmiri, L., Yakoub, S. B., & Achelhi, H. (2021). Entrepreneurial Projects' Risk Factors in Morocco. *Journal of Entrepreneurship, Business and Economics*, *9*(1), 202-229.
(23). Kerraous, E. M. (2018). How Do Moroccan Companies Incorporate Enterprise Risk Management ? Results of a Survey. *Results of a Survey (December 1, 2018)*.
(24). Kleffner, A. E., Lee, R. B., & McGannon, B. (2003). The effect of corporate governance on the use of enterprise risk management : Evidence from Canada. *Risk Management and Insurance Review*, *6*(1), 53-73.
(25). Laudon, K., & Laudon, J. (2020). *Management des systèmes d'information* (PEARSON, p. 672).
(26). Lundqvist, S. A. (2015). Why firms implement risk governance–Stepping beyond traditional risk management to enterprise risk management. *Journal of Accounting and Public Policy*, *34*(5), 441-466.
(27). M. CHOUKI, O. KHADROUF, M. TALEA, & C. OKAR. (2018). Organizational culture as a barrier of information technology adoption : The case of Moroccan Small and Medium Enterprises. *2018 IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD)*, 80-85. https://doi.org/10.1109/ITMC.2018.8691130
(28). Matrane, O., & Talea, M. (2014). A Maturity Model for Information Security Management in Small and Medium-Sized Moroccan Enterprises : An Empirical Investigation. *International Journal of Advanced Research in Computer Science*, *5*(6).
(29). Mazouni, M. H. (2008). *Pour une meilleure approche du management des risques : De la modélisation ontologique du processus accidentel au système interactif d'aide à la décision*. Institut National Polytechnique de Lorraine-INPL.
(30). Mikes, A., & Kaplan, R. S. (2014). *Towards a contingency theory of enterprise risk management*.
(31). Miller, S. E. (2009). Governance mechanisms as moderators of agency costs in a pre-SOX environment. *Journal of Business & Economics Research (JBER)*, *7*(10).
(32). MOUSSIR, C.-E., & LIOUAEDDINE, M. (2021). Impact de la formation continue sur la productivité des entreprises au Maroc : Une étude micro-économétrique. *Alternatives Managériales Economiques*, *3*(4), 299-315.

ISSN: 2658-8455
Volume 5, Issue 10 (2024), pp. 317-346.

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

(33). Nason, R. (2017). *It is not complicated : The art and science of complexity in business*. University of Toronto Press.
(34). Osipova, E. (2015). Establishing cooperative relationships and joint risk management in construction projects : Agency theory perspective. *Journal of management in engineering*, *31*(6), 05014026. https://doi.org/10.1061/(ASCE)ME.1943-5479.0000346
(35). OUFKIR, Z. A., & OUHADI, S. (2024). Firm growth in African countries : Do cultural attributes matter ? Evidence from Morocco. *IJBTSR International Journal of Business and Technology Studies and Research*, *5*(2), 12 pages-12 pages.
(36). Pagach, D., & Warr, R. (2011). The characteristics of firms that hire chief risk officers. *Journal of risk and insurance*, *78*(1), 185-211.
(37). Pradesa, H. A., Agustina, I., Taufik, N. I., & Mulyadi, D. (2021). Stakeholder Theory Perspective in the risk identification process in village government. *Jurnal Ilmu Manajemen Advantage*, *5*(1), 17-27.
(38). Raissouni, K., Errabih, Z., Charroud, S., Raissouni, R., Raissouni, M. R., & Bourekkadi, S. (2023). Cybersecurity in the Context of Moroccan Energy Companies. *E3S Web of Conferences*, *412*, 01038.
(39). Rana, T., Wickramasinghe, D., & Bracci, E. (2019). New development : Integrating risk management in management control systems—Lessons for public sector managers. *Public Money & Management*, *39*(2), 148-151. https://doi.org/10.1080/09540962.2019.1580921
(40). Siponen, M. (2000). A conceptual foundation for organizational information security awareness. Information Management & Computer Security 8(1), 31-41. *Inf. Manag. Comput. Security*, *8*, 31-41. https://doi.org/10.1108/09685220010371394
(41). Soufiane, C. (2020). Contribution à l'étude du rôle de la confiance interpersonnelle dans l'amélioration des performances individuelles des salariés au travail. *Revue Française d'Économie et de Gestion*, *1*(2).
(42). Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, *34*(1), 1-11.
(43). Thalassinos, E., Kadłubek, M., & Norena-Chavez, D. (2023). Theoretical Essence of Organisational Resilience in Management. In S. Grima, E. Thalassinos, M. Cristea, M. Kadłubek, D. Maditinos, & L. Peiseniece (Éds.), *Digital Transformation, Strategic Resilience, Cyber Security and Risk Management* (Vol. 111A, p. 133-145). Emerald Publishing Limited. https://doi.org/10.1108/S1569-37592023000111A009
(44). Vogus, T. J., & Sutcliffe, K. M. (2007). Organizational resilience : Towards a theory and research agenda. *2007 IEEE international conference on systems, man, and cybernetics*, 3418-3422.
(45). Wellalage, N. H., & Locke, S. (2011). Agency Costs, Ownership Structure and Corporate Governance Mechanisms. *Journal of Law and Governance*, *6*(3), 53-70-53-70.
(46). Yaraghi, N., & Langhe, R. G. (2011). Critical success factors for risk management systems. *Journal of Risk Research*, *14*(5), 551-581.
(47). Yin, R. K. (2018). *Case study research and applications*. Sage Thousand Oaks, CA.
(48). Zsidisin, G. A., & Ellram, L. M. (2003). An agency theory investigation of supply risk management. *Journal of Supply Chain Management*, *39*(2), 15-27.