ISSN: 2658-8455
Volume 5, Issue 1 (2024), pp. 90-102.


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

# L'audit interne des systèmes d'information au Maroc : une véritable synergie pour une cyber-sécurité

# Internal Audit of Information Systems in Morocco: A Synergy for Cybersecurity

**Yousra EL KRAMI,** ***(Docteur en Sciences de Gestion)***
*Faculté des sciences juridiques, économiques et sociales*
*Université Mohammed V de Rabat Agdal, Maroc*

**Mohamed LACHHAB,** ***(Docteur en sciences de gestion)***
*Faculté des sciences juridiques, économiques et sociales*
*Université Mohammed V de Rabat Agdal, Maroc*

**Salim EL HADDAD,** ***(Doctorant en sciences de gestion)***
*Faculté des sciences juridiques, économiques et sociales*
*Université Mohammed V de Rabat Agdal, Maroc*

| | |
|---|---|
| **Adresse de correspondance :** | Université Mohammed V/Faculté des sciences juridiques, économiques et sociales<br>Rabat, Maroc |
| **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** | EL KRAMI, Y., LACHHAB, M., & EL HADDAD, S. (2024). L'audit interne des systèmes d'information au Maroc : une véritable synergie pour une cyber-sécurité. International Journal of Accounting, Finance, Auditing, Management and Economics, 5(1), 90-102. https://doi.org/10.5281/zenodo.10547449 |
| **Licence** | **Cet article est publié en open Access sous licence CC BY-NC-ND** |

*Received: December 03, 2023* *Accepted: January 19, 2024*

# L'audit interne des systèmes d'information au Maroc : une véritable synergie pour une cyber-sécurité

## Résumé

L'audit interne des systèmes d'information revêt une importance significative pour les organisations. La synergie entre l'audit interne et les systèmes d'information a créé des opportunités pour une prise de décision plus éclairée, une meilleure capacité d'évaluation des risques et, finalement, un meilleur alignement avec les objectifs organisationnels. En effet, au-delà de ses fonctions classiques l'audit interne s'est élargi permettant ainsi d'assurer la conformité, la sécurité et l'efficacité des systèmes d'information au sein d'une organisation tout en renforçant la résilience des systèmes d'information. Notre article vise à démontrer à partir de la littérature existante l'impact de la fonction d'audit interne sur la maîtrise des risques liés à la sécurité des systèmes d'information. Pour se faire nous allons dans un premier temps définir le concept d'audit interne et l'évolution de ses fonctions, présenter l'historique relatif au renforcement du dispositif de sécurité des systèmes d'information au Maroc, démontrer comment les Outils et Techniques d'Audit Assistées par Ordinateur (CAATTs) soutiennent les processus d'audit tout en mettant en lumière la complémentarité entre l'audit interne et externe dans une logique d'audit continu. Puis nous allons mettre en exergue un ensemble d'aspects liés au développement des attributions de la fonction d'audit interne et mettre en relation l'audit interne et le Système de Management de la sécurité de l'information qui aide l'organisation à mieux gérer les risques liés à la sécurité des systèmes d'information.

**Mots clés :** Système de Management de la sécurité de l'information, audit interne, cyber-securité, Outils et Techniques d'Audit Assistées par Ordinateur.
**Classification JEL** *:* H83, M42, M4.
**Type de l'article :** article théorique

## Abstract :

Internal auditing of information systems has a significant importance for organizations. The synergy between internal audit and information systems has created opportunities for more informed decision-making, improved risk assessment and, ultimately, better alignment with organizational objectives. Indeed, beyond its traditional functions, internal auditing has expanded to ensure compliance, security and efficiency of information systems within an organization, while reinforcing the resilience of information systems. The aim of our article is to draw on existing literature to demonstrate the impact of the internal audit function on the control of information systems security risks. To do this, we will first define the concept of internal audit and the evolution of its functions, present the background to the reinforcement of information systems security in Morocco, demonstrate how Computer-Aided Audit Tools and Techniques (CAATTs) support audit processes, and highlight the complementarity between internal and external audit in a continuous audit logic. We will then highlight a series of aspects linked to the development of the internal audit function's remit, and relate internal audit to the Information Security Management System, which helps the organization to manage well the risks linked to the security of information systems.

**Keywords: (3-5 Words) :** Système de Management de la sécurité de l'information, audit interne, cyber-securité, Outils et Techniques d'Audit Assistées par Ordinateur.
**JEL Classification :** H83, M42, M4.
**Paper type:** article théorique

ISSN: 2658-8455
Volume 5, Issue 1 (2024), pp. 90-102.

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

## 1. Introduction :

L'introduction de la numérisation au sein de l'administration publique a connu une progression significative. La transformation numérique, avec son potentiel considérable, joue actuellement un rôle majeur dans la modernisation de l'ensemble des structures publiques. Malgré les avantages indéniables de la numérisation en termes de croissance économique, de souveraineté et de gouvernance efficace, elle n'est pas exempte de risques et de menaces. Pour faire face à ces défis, la cyber-sécurité a toujours été une composante essentielle des stratégies de numérisation au Maroc. L'audit interne ne cesse de s'adapter aux nouvelles applications des évolutions technologiques. En effet, si la banalisation des nouvelles technologies de l'information et de la communication (NTIC) au sein des entreprises est allée de pair avec l'émergence de nouveaux risques, comme par exemple les cyber-attaques, celle-ci a également permis le développement de nouveaux outils tels que le data analytics, le data mining, l'intelligence artificielle (P. Schick et al., 2021) et la mise en place d'un système de management de la sécurité de l'information (SMSI) pour aider l'organisation à mieux gérer les risques liés à la sécurité des systèmes d'information (SI).

Le premier pas vers une sécurité efficace implique l'identification des risques inhérents, suivi du choix de techniques de sécurité adaptées, car généralement une seule mesure de sécurité ne suffit pas. Un programme d'audit basé sur les risques contribuera à renforcer le système de sécurité organisationnel. Malgré l'importance de la relation entre l'audit interne et la sécurité de l'information et la valeur qui peut en être tirée, il n y a pas assez d'études ayant traité l'étroite relation qui réside entre les deux fonctions et sur la manière dont elles fonctionnent ensemble. Ainsi, notre article est à visée descriptif en vue d'enrichir la littérature existante concernant ces fonctions complémentaires mais qui s'avèrent nécessaire dans un environnement marqué par l'accroissement significatif des risques SI.

En outre, des études relèvent que les auditeurs consacrent la majeure partie de leur temps aux activités d'assurance au détriment des activités de conseil. De nos jours, l'audit interne revêt des fonctions bien plus larges et se concentrera plus sur l'audit des processus opérationnels, l'audit de conformité et de régularité, ainsi que sur l'audit des risques financiers et des systèmes d'information. La question qui est au cœur de notre recherche est quel est l'impact de la fonction d'audit interne sur la maîtrise des risques liés à la sécurité des systèmes d'information ?

Afin d'apporter des éléments de réponses à cette question nous avons jugé essentiel de définir la fonction d'audit interne, de présenter le cadre réglementaire et le contexte dans lequel la sécurité des SI est devenue une nécessité au Maroc. Etant donné l'accélération du processus de digitalisation nous allons démontrer dans quelle mesure l'audit interne renforce la sécurité des systèmes d'informations tout en mettant l'accent sur deux composantes essentielles à savoir l'importance de la mise en place d'un SMSI et les techniques d'audit assistées par ordinateur qui ont accompagnés la digitalisation de la fonction.

## 2. Contexte général et cadre réglementaire de la sécurité des SI au Maroc :

Dans un contexte marqué par l'évolution croissante de la digitalisation et du numérique le Maroc a fait le choix, sous la conduite éclairée des hautes orientations royales d'accorder une importance particulière aux nouvelles technologies de l'information et des communications (NTIC), eu égard à leur rôle fondamental en matière de développement socio-économique. La dynamique enregistrée pour l'accélération de la transition numérique nationale s'est vue appuyée par le nouveau modèle de développement qui a consacré le digital comme levier transverse pour un développement plus inclusif et responsable.

Dans cette perspective, une initiative soutenue a été lancée depuis la création de la Direction Générale de la Sécurité des Systèmes d'Information (DGSSI). En 2014, une première version de la Directive Nationale de la Sécurité des Systèmes d'Information (DNSSI) a été émise par le biais de la circulaire N° 3/2014 du Chef du Gouvernement. En 2020, la législation nationale a été renforcée par l'adoption de la loi n° 05-20 relative à la cyber-sécurité, suivie en 2021 par le décret n° 2-21-406 qui en précise l'application. Pour s'adapter à l'évolution constante de l'environnement des technologies de l'information et des menaces associées, la DGSSI a mis à jour la Directive Nationale de la Sécurité des Systèmes d'Information dans sa version 2.0, conformément aux directives royales. Ainsi, le Chef du gouvernement a diffusé la circulaire 02/2023 auprès des entités et des infrastructures d'importance vitale (IIV), fixant comme délai six mois à compter de la date de sa publication pour l'élaboration d'un plan d'action visant à se conformer aux nouvelles exigences de sécurité.

Ce qui a suscité l'implication de tous les acteurs publics, à savoir, les administrations publiques, les entreprises et établissements publiques (EEP) en vue de s'inscrire dans ce chantier novateur de protection des systèmes d'information. L'audit interne est l'outil le plus répandu pour vérifier, évaluer et améliorer l'efficacité d'un système de management de la sécurité de l'information (SMSI). Son objet n'est en aucun cas de trouver les points faibles de l'organisation mais de s'inscrire dans une perspective d'amélioration continue.

## 3. Concept d'audit interne :

L'audit interne est entré de plain-pied dans le XXIe siècle, (Renard jacques ,2017). D'abord fonction à caractère confidentiel aux contours incertains, limité aux grandes entreprises, elle est devenue en quelques décennies un des piliers essentiels dans la gouvernance des organisations de toutes tailles et de toute nature. L'IIA (Institute of Internal Auditors) et le Conseil d'administration de l'IFACI ont approuvé en 1999 la définition suivante de l'audit interne : L'audit interne est une activité objective et indépendante qui assure aux organisations un degré de maîtrise des opérations, c'est une fonction qui permet de relever les dysfonctionnements et émet des conseils pour pallier à ces anomalies. Elle est également créatrice de valeur ajoutée dans la mesure où elle contribue à l'atteinte des objectifs fixés en évaluant, par une approche méthodique et systématique, ses processus de gestion des risques, de gouvernance et de contrôle par le biais de recommandations pour renforcer leur efficacité. Cette fonction aux attributions transversales accompagne l'organisation dans son processus de pilotage stratégique, elle renforce sa gouvernance et contribue à l'amélioration de sa performance. Devenue essentielle à la survie de tous les organismes qu'ils soient public ou privé, la FAI doit respecter au maximum les normes internationales mises en vigueur et les principes instaurés.

Au-delà de ses fonctions traditionnelles, l'auditeur interne examine entre autres quels sont les indicateurs, les systèmes d'information utilisés et quelles mesures peuvent être prises en compte pour que les dispositions, règles, procédures, etc. soient mieux adaptées.

Ce document évalue le rôle des technologies de l'information et la manière dont elles affectent le processus d'audit interne dans l'organisation. L'étude met également l'accent sur la tendance mondiale à l'adoption de systèmes informatiques (logiciels/matériels) pour créer un environnement plus contrôlé dans le cadre du processus d'audit. Elle montre également comment les technologies de l'information affectent le contrôle interne (environnement de contrôle, évaluation des risques, activités de contrôle, information, communication et suivi) et fournit des lignes directrices et des bonnes pratiques pour évaluer les techniques disponibles afin d'effectuer efficacement les tâches d'audit en interne. Il traite également de la manière dont la technologie, les systèmes d'information (SI) et le traitement électronique des données (TED) ont modifié la façon dont les organisations mènent leurs activités, en promouvant

ISSN: 2658-8455
Volume 5, Issue 1 (2024), pp. 90-102.

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

l'efficacité opérationnelle et en aidant à la prise de décision. Il met également en lumière de nombreux aspects des risques et des contrôles informatiques et indique si les bonnes personnes supervisent les risques informatiques comme elles le devraient. Il démontre l'impact de la convergence des technologies sur le mécanisme de contrôle interne d'une entreprise. Il souligne que l'auditeur a également la responsabilité de s'assurer que le niveau de gouvernance de la direction (le comité d'audit et le conseil d'administration) comprend les risques acceptés par la direction et les responsabilités potentiellement transférées aux membres du conseil d'administration.

## 4. Les techniques d'audit assistées par ordinateur (CAATTs) :

De nos jours, les processus d'audit sont soutenus par plusieurs Outils et Techniques d'Audit Assistées par Ordinateur (CAATTs). Les CAATTs peuvent être définis comme "tout usage de la technologie visant à faciliter l'achèvement d'un audit. Cette définition large inclurait les travaux automatisés et les applications traditionnelles de traitement de texte (L Braun. et al 2003), ou comme l'utilisation de certains logiciels pouvant être utilisés par l'auditeur pour effectuer des audits et atteindre les objectifs de l'audit (S. A. Sayana, 2003).
Les CAATTs (Computer Assisted Audit Tools) peuvent être classés "dans quatre grandes catégories : logiciels d'analyse de données ; logiciels/utilitaires d'évaluation de la sécurité du réseau ; logiciels/utilitaires d'évaluation de la sécurité des systèmes d'exploitation (OS) et des systèmes de gestion de bases de données (DBMS) ; outils de test de logiciels et de code (S. A. Sayana, 2003). Nous pouvons inclure IDEA (Interactive Data Extraction and Analysis) et ACL (Audit Command Language) dans la première catégorie, et, parmi leurs principales utilisations, ces outils peuvent être utilisés pour la détection de fraudes : des preuves sont recueillies par des entretiens, l'examen de documents et l'utilisation de CAAT (M. Popa et al, 2009).
Dans ce sens, on pourrait dire que l'audit interne et la sécurité des systèmes d'information sont complémentaires et que les entités d'audit interne et des systèmes d'information peuvent travailler en synergie pour mener à bien la sécurité des systèmes d'information. De plus, (Dai et Vasarhelyi, 2017) ont documenté des preuves qui soutiennent une relation positive entre la technologie de surveillance du contrôle interne et l'efficacité de l'audit dans les contextes d'audit interne et externe.

## 5. L'audit interne et externe à l'épreuve de l'audit continu

Eu égard à ses objectifs, l'audit externe englobe tout ce qui concourt à la détermination des résultats, à l'élaboration des états financiers et rien que cela ; mais dans toutes les fonctions de l'entreprise. L'auditeur externe qui limiterait ses observations et investigations au secteur comptable ferait œuvre incomplète. Les professionnels le savent bien qui explorent toutes les fonctions de l'entreprise et tous les systèmes d'information qui participent à la détermination du résultat et cette exigence est de plus en plus grande au fur et à mesure que se développent les saisies à la source. L'audit interne quant à lui est beaucoup plus vaste puisqu'il inclut non seulement toutes les fonctions de l'entreprise, mais également toutes les dimensions de l'entreprise.
Le concept d'audit continu a vu le jour il y a plus de vingt ans. Pourtant, malgré les avantages qu'on lui prête, son acceptation et son utilisation dans la pratique ont été lentes. Pour mieux comprendre la situation, une étude (George C. Gonzalez et al. 2012) a été menée auprès de 210 auditeurs internes du monde entier sur leur utilisation de l'audit continu. En utilisant la théorie unifiée de l'acceptation et de l'utilisation des technologies (UTAUT), ils ont exploré les antécédents des intentions des auditeurs internes d'utiliser la technologie de l'audit continu.

Ainsi, il a été constaté que les auditeurs internes d'Amérique du Nord sont plus susceptibles d'utiliser l'audit continu en raison des pressions sociales douces de l'influence sociale exercée par les pairs et les autorités supérieures. En revanche, les auditeurs du Moyen-Orient sont plus enclins à utiliser cette technologie si elle est imposée par les autorités supérieures.

Ainsi, la notion d'audit continu a été mise à l'épreuve, ce concept a été présenté comme offrant de nombreux avantages importants aux organisations, notamment la réduction des erreurs comptables, une analyse plus rapide et une communication organisationnelle plus opportune, ainsi qu'une efficacité accrue de l'audit. Plusieurs études de recherche ont mis en avant ces avantages (Vasarhelyi et al., 2004 ; Kuhn et Sutton, 2006), ils ont exploré les aspects techniques de la mise en œuvre de la technologie d'audit continu (Kuhn et Sutton, 2010), étudié les mises en œuvre réelles en pratique (Hermanson et al., 2006) et examiné les effets psychologiques de l'audit continu sur les gestionnaires (Hunton et al., 2008 ; Hunton et al., 2010). Malgré le fait que le concept existe depuis environ deux décennies, introduit par Groomer et Murthy (1989) et Vasarhelyi et Halper (1991), la mise en œuvre pratique de l'audit continu a été plus l'exception que la règle.

Jusqu'à présent, l'utilisation de la technologie d'audit continu a été presque exclusivement limitée à la fonction d'audit interne (Chan and Vasarhelyi, 2011). Depuis 2005, certaines des plus grandes firmes comptables internationales ont interrogé les directeurs de l'audit et d'autres responsables principaux de l'audit interne de leurs clients pour comprendre leurs pratiques en matière d'audit continu (PricewaterhouseCoopers (PricewaterhouseCoopers (PwC), 2007, KPMG International (KPMG), 2010, Grant Thornton, 2011). Les résultats de ces enquêtes varient en termes de l'étendue de l'utilisation effective de l'audit continu (George C. Gonzalez & al. 2012). Par exemple, une enquête a révélé que, parmi les clients de la firme comptable interrogée, 13% disposaient d'un système d'audit continu pleinement opérationnel et 37% avaient un système en place mais pas encore pleinement développé (PwC, 2006). Une autre enquête menée par une autre firme indiquait des chiffres de 7% et 13%, respectivement (KPMG, 2010). Cependant, quel que soit le niveau d'utilisation de l'audit continu, les répondants s'attendent à un niveau d'utilisation beaucoup plus élevé dans deux ans avec une progression continue.

Par ailleurs, de nombreux scandales passés et les réglementations qui en ont résulté ont joué un rôle déterminant dans l'adoption de l'audit continu (Cullinan, 2004). Aux États-Unis, en particulier, l'adoption de l'audit continu a été largement motivée par la promulgation de la loi Sarbanes-Oxley. Une fois mis en place, les systèmes d'audit continu ont la capacité de fournir des informations fiables aux auditeurs tout en optimisant l'utilisation des ressources. En théorie, ces systèmes peuvent aboutir à des audits plus efficaces en offrant des informations financières pertinentes et fiables en temps réel. Il est observé que les auditeurs externes ont tendance à accorder une plus grande confiance au travail de l'audit interne lorsqu'ils utilisent des systèmes d'audit continu plutôt que des systèmes traditionnels, renforçant ainsi l'efficacité globale des audits (Kim et al., 2009).

Les auditeurs internes et externes sont indirectement, voire directement, un mécanisme de contrôle de l'entité qui garantit que les attentes en matière de conformité sont correctement prises en compte par la direction. L'importance de la sécurité de l'information est d'autant plus grande eu égard au nombre de lois relatives à la protection des actifs informationnels et de réglementations qui ont un impact sur les attentes en matière de conformité. L'assurance de la conformité constitue pour la plupart des entités un objectif d'audit important en matière de sécurité de l'information et la meilleure façon d'y parvenir est de procéder à un audit continu des incidents liés à la sécurité de l'information.

Par conséquent, un auditeur doit vérifier en permanence si des procédures efficaces de protection du patrimoine informationnel sont mises en œuvre pour gérer et maintenir la sécurité de l'information tout au long du cycle de vie de l'information (R.Davis, 2012).

ISSN: 2658-8455
Volume 5, Issue 1 (2024), pp. 90-102.

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

## 6. L'importance de la mise en place d'un SMSI :

Malgré des avancées significatives dans le domaine de la sécurité de l'information, tels que le modèle de matrice d'accès sujet/objet, les listes de contrôle d'accès, la sécurité multiniveau utilisant le flux d'information et la propriété en étoile, la cryptographie à clé publique et le protocole cryptographique, de nombreux systèmes d'information sont vulnérables aux attaques internes ou externes (Butler W. Lampson, 2004). La mise en place de la sécurité prend du temps et ne contribue en rien à l'obtention de résultats utiles. Si la configuration est trop permissive, personne ne s'en apercevra à moins qu'un audit soit déjà mis en place. Cette observation met en évidence la nécessité d'un audit interne pour la sécurité des systèmes d'information dans chaque organisation. Il existe trois domaines d'activité informatique doivent être contrôlés régulièrement, le contrôle de l'accès des utilisateurs, la surveillance de l'activité du système et la piste d'audit (Mukaila Apata, 2010).

L'objectif de la sécurité dans le domaine du contrôle d'accès des utilisateurs est d'optimiser et de réduire les risques d'erreur et de fraude, d'éliminer les accès non autorisés et de garantir la confidentialité des données. Il est également évident de surveiller en permanence l'activité du système car les actes malveillants ou de fraude sont plus susceptibles de se produire s'il y a peu de chances de les détecter (Ana-Maria SUDUC et al., 2010).

Il est crucial de reconnaître l'évolution du champ d'intervention de la fonction d'audit interne afin de préparer le terrain pour la discussion ultérieure sur le rôle des systèmes d'information dans la gestion de l'activité d'audit interne. Historiquement considéré comme une fonction isolée axée sur la conformité et la communication financière, l'audit interne a dépassé ses limites traditionnelles pour jouer un rôle plus stratégique dans la gestion des risques organisationnels. Les progrès dans les systèmes d'information ont joué un rôle crucial dans cette transformation. Les systèmes d'information constituent l'épine dorsale qui permet aux entités d'audit interne d'exécuter des tâches complexes, allant de la planification à la documentation et à la communication des audits. Ces systèmes abordent les défis liés à la gestion de vastes ensembles de données, de multiples processus et des environnements réglementaires en constante évolution.

La synergie entre l'audit interne et les systèmes d'information a créé des opportunités pour une prise de décision plus éclairée, une meilleure capacité d'évaluation des risques et, finalement, un meilleur alignement avec les objectifs organisationnels. Elle explore le rôle crucial des systèmes d'information dans la gestion de l'audit interne, en mettant principalement l'accent sur les étapes de planification, de documentation et de communication.

Conformément à la norme ISO 27001, l'audit interne représente une fonction cruciale au sein d'un système de management de la sécurité de l'information (SMSI), sa mise en œuvre, exigée par la clause 9.2 de la norme ISO 27001, peut s'avérer complexe, surtout pour les petites organisations, en raison de la nécessité de disposer de ressources indépendantes du développement et de la maintenance du SMSI, possédant les compétences requises pour assurer la fonction d'auditeur interne.

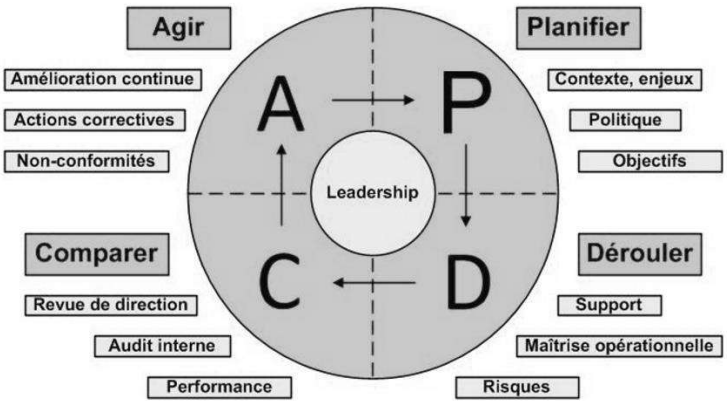
Ce type d'audit implique une évaluation approfondie du SMSI de l'organisation afin de garantir sa conformité aux critères de la norme. Chaque exigence de la norme doit être rigoureusement vérifiée, avec des preuves à l'appui. Contrairement à une évaluation de certification, l'audit interne peut être réalisé par le personnel interne de l'organisation ou par une société externe, tout en garantissant l'indépendance des auditeurs.

L'audit interne ISO 27001 permet d'identifier d'éventuelles non-conformités nécessitant une attention particulière, contribuant ainsi à l'amélioration continue du SMSI. Les résultats de l'audit doivent être analysés lors des revues de direction. La clause 9.2 de la norme ISO 27001 stipule l'obligation pour l'organisation d'effectuer des audits internes à des intervalles planifiés. Ces audits fournissent des informations sur la conformité du SMSI aux exigences

spécifiques de l'organisation et de la norme. Des exigences additionnelles, détaillées dans cette clause, sont également documentées.

La chaîne Planifier-Mettre en œuvre-Contrôler-Améliorer **« Plan-Do-Check-Act »** est utilisée par la norme ISO 27001 pour la mise en œuvre du SMSI et repose sur l'idée d'un processus continu de mise en place de la sécurité de l'information (Stefan F, et al. 2007).

***Figure 1 : Le cycle PDCA de la roue de Deming.***




***Source : Le cycle PDCA de Deming, Exigences de la norme ISO 27001.***

## 7. Les étapes d'audit interne d'un système d'information

Selon la norme ISO 19011- 2018 relative aux lignes directrices pour l'audit des systèmes de management, une mission d'audit interne des systèmes d'information suit généralement plusieurs phases, durant la phase de déclenchement et de préparation de l'audit, la mission débute par l'établissement d'une lettre de mission, signée par le demandeur et définissant les objectifs, le périmètre, les critères d'audit, les circuits de communication, et les ressources nécessaires. Une équipe d'audit est constituée, et le prestataire doit nommer un responsable d'audit. L'organisme audité doit fournir la documentation requise, et une convention d'audit, comprenant les objectifs, critères, dates, et lieux, doit être établie et signée.

Ensuite, la phase de préparation de l'audit implique la création d'un plan de charge d'audit, couvrant les objectifs, le périmètre, les critères, la démarche, les activités, et le planning prévisionnel. L'équipe d'audit élabore la stratégie de tests, incluant une revue documentaire et des scénarios de tests techniques.

La phase d'exécution de l'audit et d'analyse des constats comprend une réunion d'ouverture pour valider le plan de charge, exposer le planning, présenter les activités d'audit, et clarifier les communications. Les livrables incluent un plan d'assurance qualité, une note de cadrage, et un planning prévisionnel. L'exécution des tests prévus a lieu, et les enregistrements de cette phase comprennent les constats des auditeurs, les recommandations, les engagements de l'organisme audité, et les relevés techniques.

La phase de clôture nécessite la rédaction du rapport d'audit par le prestataire, suivi d'une réunion de clôture pour présenter le rapport à la direction de l'organisme audité. Le rapport doit être émis dans les délais convenus, rester confidentiel, et marquer la fin de la mission après la réalisation des actions définies dans le plan de charge d'audit. Des actions correctives peuvent être incluses dans les conclusions, avec un suivi de leur mise en œuvre, rapporté au commanditaire de l'audit.

Les livrables de la phase de clôture, tels qu'une politique de sécurité, une charte d'utilisation des ressources SI, une matrice des risques SI, et un cahier des charges des solutions retenues, sont discutés et fixés au début de la mission.

Dans le cadre de la norme SAS n° 94, l'AICPA précise les facteurs que les auditeurs doivent prendre en considération dans le processus d'audit des états financiers et son implication dans

ISSN: 2658-8455
Volume 5, Issue 1 (2024), pp. 90-102.

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

les audits d'entreprises de toutes tailles. Les auteurs ont également examiné et discuté les cinq aspects les plus importants de la norme n° 94, ce que confirme Tucker (2001). En outre, le SAS n° 94 reconnaît les types de systèmes, de contrôles et d'éléments probants auxquels les auditeurs sont confrontés. L'auteur a brièvement abordé le Statement Of Information System Auditing (SISA), qui définit les exigences obligatoires en matière d'audit des systèmes d'information et d'établissement de rapports. Il passe en revue les normes SISA 010 à SISA 080. Les auteurs ont fourni des explications détaillées sur les normes et lignes directrices d'audit disponibles aux États-Unis et suggèrent comment ces normes et lignes directrices peuvent fondamentalement aider les auditeurs dans l'audit des systèmes d'information. Toutefois, ils n'ont pas précisé le type d'application de l'audit informatique et la manière dont il affecte directement la profession d'auditeur. Ils n'ont pas non plus démontré l'importance de l'impact de la technologie sur les rôles et les responsabilités des auditeurs.

## 8. La relation entre l'audit interne et la sécurité des systèmes d'information

L'audit interne représente un processus développé pour identifier les forces et les faiblesses des organisations. Ainsi, l'adoption de fonctionnalités technologiques représente un facteur favorisant les processus liés à la minimisation des coûts et à la maximisation des revenus. De plus, les pressions croissantes des régulateurs concernent de nouveaux défis, à savoir, la protection des données, la communication non financière et les risques cybernétiques, imposant l'adoption de dispositifs numériques (Simone Pizzi et al., 2021). Les évolutions dans les technologies de l'information ont également grandement affecté la profession de l'audit interne. Avec l'utilisation généralisée de plateformes informatiques d'entreprise, les preuves d'audit et les points de contrôle qui étaient autrefois sous forme papier sont désormais électroniques (Bierstaker et al., 2001). En raison de l'utilisation des technologies de l'information dans l'exécution des activités quotidiennes des entreprises, les auditeurs sont désormais tenus de recueillir et d'évaluer électroniquement les preuves (Boydaş, 2013). Par conséquent, en plus des procédures d'audit traditionnelles, des méthodes d'audit basées sur l'utilisation de la technologie ont également commencé à être employées aujourd'hui (Menna et al., 2016).

Les fonctions d'audit interne et de sécurité de l'information devraient travailler en synergie, le personnel chargé de la sécurité de l'information conçoit, met en œuvre et exploite diverses procédures et technologies pour protéger les ressources d'information de l'organisation, et l'audit interne fournit un retour d'information périodique sur l'efficacité de ces activités, ainsi que des suggestions d'amélioration (Y.RACHIDI & M.LAHMOUCHI, 2018).

La sécurité de l'information est nécessaire non seulement pour protéger les ressources d'une organisation, mais aussi pour garantir la fiabilité de ses états financiers et autres rapports de gestion (AICPA et ICCA, 2008). Par conséquent, COBIT4 (ITGI 2007), un cadre normatif pour le contrôle et la gouvernance des technologies de l'information, souligne que la conception et la mise en œuvre d'un programme de sécurité de l'information rentable font partie des responsabilités de la direction en matière de gouvernance. En conséquence, les chercheurs en SI ont commencé à étudier les différentes dimensions de la gouvernance de la sécurité de l'information. Un premier courant de recherche s'est concentré sur la mesure de la valeur des investissements dans la sécurité de l'information (Gordon et al., 2003, Cavusoglu et al., 2004a, Iheagwara, 2004Bodin et al., 2008, Kumar et al., 2008). Un deuxième courant de recherche a examiné les réactions des marchés boursiers à la divulgation d'initiatives en matière de sécurité de l'information (Gordon et al. 2010) et d'incidents (Campbell et al., 2003, Cavusoglu et al., 2004). Un troisième courant de recherche a examiné les moyens d'améliorer la conformité des utilisateurs finaux aux politiques de sécurité de l'information d'une

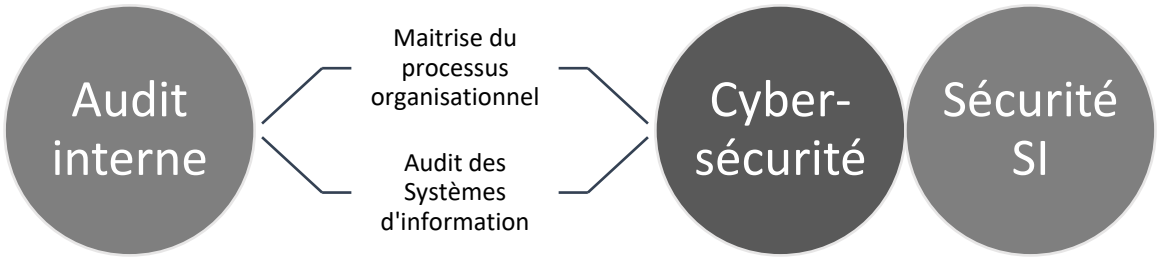
organisation (D'Arcy et al., 2009, Bulgurcu et al., 2010, Johnston et Warkentin, 2010, Siponen et Vance, 2010,). De plus une enquête élaborée par le cabinet KPMG France a démontré que les auditeurs internes et les responsables cyber-sécurité partagent le même avis et estiment que le risque cyber est majeur, voire critique pour leur organisation. Une vision que la crise sanitaire n'a pas accentuée de manière significative. Pour les deux populations, la résilience des moyens technologiques et la protection contre les cyberattaques seront les principaux enjeux à prendre en compte dans les années à venir.

Les responsables de la cyber-sécurité et les auditeurs internes s'accordent sur le fait que la divulgation d'informations confidentielles et les atteintes à la réputation sont les deux impacts cyber les plus redoutés. Cependant, dans un contexte marqué par une augmentation des menaces, de la surface d'exposition et des réglementations, les responsables de la cybersécurité se concentrent principalement sur les enjeux opérationnels liés à la continuité de l'activité et à l'intégrité des données. En revanche, les auditeurs internes accordent une plus grande importance aux exigences réglementaires.

Plus de trois quarts des auditeurs internes déclarent auditer des sujets liés à la cybersécurité, une proportion qui ne cesse d'augmenter depuis quatre ans. Les tests d'intrusion et l'analyse de données sont désormais largement utilisés par la majorité des auditeurs internes, en complément des approches traditionnelles telles que les entretiens, l'analyse documentaire et les tests de cheminement. Les responsables de la cybersécurité, quant à eux, privilégient les tests d'intrusion, les campagnes de phishing et les revues de code, de configuration ou d'architecture.

Ainsi, il convient de noter qu'en plus de la maîtrise du processus organisationnel, la fonction d'audit interne a élargi au fil du temps son champ d'intervention en s'intéressant à l'audit des systèmes d'information pour contribuer au renforcement de la cyber-sécurité et assurer la sécurité des systèmes d'information.

***Figure 2 : l'interrelation entre l'audit interne et la sécurité des systèmes d'information***




***Source : élaborée par nos soins.***

## 9. L'impact de l'audit interne sur la sécurité des systèmes d'information :

La littérature abonde en arguments soutenant l'importance de l'audit interne des SI et met en lumière l'impact positif qui réside entre les deux fonctions. Voici quelques points clés issus de la littérature :

- La conformité et Normes de Sécurité : La mise en place d'un SMSI, conforme à des normes internationales telles qu'ISO 27001, fournit un cadre solide pour garantir la conformité aux réglementations en matière de sécurité de l'information.
- Identification et gestion des risques : le SMSI facilite l'identification proactive des risques liés à la sécurité de l'information au sein de l'organisation. L'audit interne permet ensuite d'évaluer l'efficacité des mesures de gestion des risques mises en place.

ISSN: 2658-8455
Volume 5, Issue 1 (2024), pp. 90-102.

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

- Renforcement de la résilience : en évaluant régulièrement la résilience des SI à travers des audits internes, les organisations peuvent identifier les faiblesses potentielles et mettre en œuvre des mesures correctives pour renforcer leur capacité à faire face aux incidents de sécurité.
- Optimisation des processus : l'audit interne des SI permet d'identifier les lacunes dans les processus et les procédures liés à la sécurité de l'information, ce qui contribue à les optimiser pour une meilleure efficacité opérationnelle.
- Sensibilisation et culture de la sécurité : les audits internes servent également à évaluer le niveau de sensibilisation à la sécurité au sein de l'organisation. Ils peuvent contribuer à renforcer une culture de la sécurité en soulignant l'importance de la sécurité de l'information à tous les niveaux.
- Évaluation de la conformité aux politiques internes : l'audit interne permet de s'assurer que les politiques internes de sécurité de l'information sont respectées, ce qui est essentiel pour maintenir un environnement informatique sûr.
- Réponse aux incidents : en testant la préparation de l'organisation à répondre aux incidents de sécurité, l'audit interne contribue à améliorer les plans de réponse aux incidents.

## 10.Conclusion :

En définitif, les fonctions d'audit interne et de sécurité de l'information devraient travailler en synergie, le personnel chargé de la sécurité de l'information conçoit, met en œuvre et exploite diverses procédures et technologies pour protéger les ressources informationnelles de l'organisation, et l'audit interne fournit un retour périodique sur l'efficacité de ces activités, ainsi que des suggestions d'amélioration.

Les risques contemporains requièrent l'usage d'applicatifs de plus en plus sophistiqués. Dans la première partie de l'article, nous avons indiqué que l'environnement de l'audit a évolué tant en termes d'objectifs qu'en termes de périmètre audité, nous conduisant de l'audit des comptes vers un audit plus large des organisations, des risques et des systèmes d'information. Il est très important de garantir un niveau acceptable de cyber sécurité dans les institutions publiques d'où la nécessité obligatoire de la mise en œuvre et de la certification selon des normes internationales. Ainsi plusieurs études ont été élaborées dans ce sens et sur la base des résultats obtenus, une série de recommandations ont été émises, comprenant la création de systèmes de gestion de la sécurité de l'information (SGSI), la réalisation d'audits internes et externes des systèmes pour répondre aux tendances, ainsi que l'alignement aux exigences obligatoires en matière de sécurité cybernétique (Arina. A, 2021).

Les recherches futures devraient viser à identifier les facteurs influençant la mise en place effective d'un audit interne des systèmes d'information qui est devenue de nos jours une nécessité fondamentale.

L'audit interne des systèmes d'information (SI) est effectivement crucial pour garantir la conformité, la sécurité et l'efficacité des SI au sein des organisations. La mise en place d'un Système de Management de la Sécurité de l'Information (SMSI) contribue à renforcer la résilience des SI en fournissant un cadre structuré pour identifier, évaluer et traiter les risques liés à la sécurité de l'information.

**Références :**


(1). A.DURDU, I.ÇINAR, Ö.CANAY. (2023) Utilization of Information Systems to Enhance the Efficiency of Internal Audit Activity Management and Audit Testing Processes, BIDGE Publications, p : 310-320.

(2). A.M. SUDUC, M. BIZOI, F.G FILIP (2010) Audit for Information Systems Security. Valahia University of Targoviste, Romanian Academy-INCE & BAR, Bucharest, p : 44-45.

(3). Arina Alexei. (2021), Ensuring information security in public organizations in the republic of Moldova Through the ISO 27001 Standard, Journal of Social Sciences, Vol. 4, p : 86-87.

(4). Bierstaker, J.L., Burnaby, P. & Thibodeau, J. (2001). "The impact of information technology on the audit process: an assessment of the state of the art and implications for the future," Managerial Auditing Journal, Vol. 16 No. 3, pp. 159–164.

(5). Butler W. Lampson bu, (2004) Computer Security in the Real World. In Proceedings of the Annual Computer Security Applications Conference, p : 37-38.

(6). Cullinan, C. (2004). Enron as a symptom of audit process breakdown : Can the Sarbanes Oxley Act cure the disease ? Critical Perspectives on Accounting, p : 853-864.

(7). D. Chan et al. (2011) Innovation and practice of continuous auditing. International Journal of Accounting Information System.

(8). Dai.J & Vasarhelyi, M. (2017), Toward blockchain based accounting and assurance, Journal of information systems.

(9). DGSSI (2015), Guide d'Audit de la Sécurité des Systèmes d'Information.

(10). E. E. Mandzila. (2004), La contribution du contrôle interne et de l'audit au gouvernement de l'entreprise. Gestion et management. Thèse pour l'obtention du doctorat, Université Paris XII Val de Marne.

(11). George C. Gonzalez & al. (2012), The antecedents of the use of continuous auditing in the internal auditing context, International Journal of Accounting Information Systems

(12). Groomer S.M. et al. (1989) Continuous auditing of database applications: an embedded audit module approach J. Inf. Syst.

(13). ISO/IEC 27001:2022. (2023, February 2). ISO. https://www.iso.org/standard/27001

(14). J. Hunton et al. (2010) Continuous monitoring and the status quo effect Int J Account Inf Syst.

(15). J.Steinbart, Robyn L. Raschke, Graham Gal, William N. Dilla, (2012), The relationship between internal audit and information security : An exploratory investigation, International Journal of Accounting Information Systems, p : 228-243, Volume 13, Issue 3.

(16). Jougier. (2022, December 8). Clause 9.2 : Audit interne ISO 27001. Protectam. https://protectam.fr/iso-27001/clause-9-2-audit-interne-iso-27001/

(17). Kim, H. J., Mannino, M., & Nieschwietz, R. J. (2009). Information technology acceptance in the internal audit profession : Impact of technology features and complexity. International Journal of Accounting Information Systems, p : 214-228.

(18). Luay Daouda & al, (2021) Contents lists available at Growing Science Accounting homepage : Moderating the role of top management commitment in usage of computer-assisted auditing techniques, Accounting Department, BINUS Online Learning, Bina Nusantara University, Jl. Kyai H. Syahdan No.9, p : 457–468.

(19). M. Apata. (2010), The Essence of Information System Security and Audit.

(20). M. Krishna Moorthy & al., (2011), The impact of information technology on internal auditing African Journal of Business Management Vol. 5, p : 3525-3527.

ISSN: 2658-8455
Volume 5, Issue 1 (2024), pp. 90-102.

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

(21). M. Popa et al, (2009), Characteristics of the Audit Processes for Distributed Informatics Systems. Informatica Economică, Volume 13, Number 3.
(22). Menna, T., Mohamed, E. K., Hussain, M., & Mohamed, B. (2016). The implication of information technology on the audit profession in developing country, International Journal of Accounting & Information Management, 25 (2), 2017, 237–255.
(23). Mohammed ALKEBSI & Khairul AZMAN AZIZ. (2017), Information Technology Usage, Top Management Support and Internal Audit Effectiveness, Asian Journal of Accounting and Governance, p: 123–132.
(24). P.Shick, J. Vera, O. Bourrouilh-Parège (2021) Audit interne et référentiels de risques : vers la maîtrise des risques et la performance de l'audit, Dunod, p : 42-53.
(25). R. L Braun. et al. (2003), Computer-assisted audit tools and techniques : Analysis and perspectives, Managerial Auditing Journal, Vol. 18, Issue 9, p : 725-731.
(26). Raad Oleiwi, (2023) The extent to which textbooks fulfill the requirements of digital transformation in accounting and auditing, International Journal of professional Business review.
(27). Robert E. Davis (2012), The Case for Continuous Auditing of Management Information System, Q-Finance, p : 6-7.
(28). S. A. Sayana (2003), Using CAATTs to Support IS Audit, Information Systems Control Journal, Volume 1.
(29). Simone Pizzi., et al. (2021) Technology in Society, Assessing the impacts of digital transformation on internal auditing: A bibliometric analysis, Volume 67, p : 14-15.
(30). Tan Pei Tong & al, (2023) The impact of forensic accounting tools in investigating white-collar crime E3S Web of Conferences.
(31). The IT Governance Institute (ITGI, Hrsg.) (2007) COBIT 4.1. Stefan F., Gernot G., Andreas E., Bernhard R., Edgar W. (2007) Information Security Fortification by Ontological Mapping of the ISO/IEC 27001 Standard. In : 13th Pacific Rim International Symposium on Dependable Computing (PRDC), Melbourne, Australia, p. 381-388.
(32). Vasarhelyi & al. (1991), The continuous process audit system : a unix- based auditing, the EDP Auditor journal, Vol III, p : 85.
(33). Volume 13, Issue 3, September 2012, p : 248-262.
(34). Y.RACHID & M.LAHMOUCHI. (2018), Internal control practices in a Moroccan public enterprise: A case study, Asia Life Sciences, p : 275-290.