

L'évaluation du système de management de la sécurité de l'information (SMSI) Aux normes internationales iso 27001 : Étude de cas de l'entreprise portuaire de Skikda. -Algérie-

تقييم نظام إدارة أمن المعلومات وفق المعايير الدولية إيزو 27001 دراسة حالة المؤسسة المينائية بسكيكدة. - الجزائر -

The evaluation of the information security management system (ISMS) In accordance with international standards iso 27001: Case study of the port company of Skikda -Algeria-

MEKIMAH Sabri^{1*}; ZERDOUDI Amina²

Date de réception : 07/ 04/ 2020 - Date d'acceptation : 04/ 01/ 2021 - Date d'édition : 01/ 06/ 2022

ملخص:

تهدف هذه الدراسة إلى تشخيص واقع تطبيق نظام إدارة أمن المعلومات وفق معيار إيزو 27001 بالمؤسسة المينائية بسكيكدة، كنموذج عن للمؤسسات الاقتصادية بالجزائر، ومن أجل الإجابة على الإشكالية وتحقيق أهدافها تم استخدام المنهج الوصفي التحليلي، كما تم الاعتماد على الاستبيان، تم توزيعه على عينة عشوائية من عمال المؤسسة البالغ عددهم 107 موظف، وذلك لتقييم مدى تطابق إدارة أمن المعلومات بالمؤسسة مع نظام إيزو 27001، وكذلك تحديد نقاط القوة والضعف في النظام الداخلي المطبق بالمؤسسة المينائية. توصلت الدراسة إلى نتائج جد مهمة متمثلة في تحديد نسبة تطبيق إجمالية لمتطلبات نظام إدارة أمن المعلومات وفق إيزو 27001 قدرها 67.14% وهي نسبة تطبيق متوسطة، ولتحسين هذه النسبة نوصي بضرورة تبني نظام إدارة أمن المعلومات لتزويد المشاركين والفاعلين بالمؤسسة بالمهارات اللازمة للإجراء المراجعات الداخلية على أنظمة إدارة سلامة المعلومات والمساهمة في التحسين المستمر من أجل تهيئة الأرضية للحصول على شهادة الايزو 27001. **الكلمات الدالة:** أمن المعلومات، إدارة أمن المعلومات، نظام إيزو ISO27001، متطلبات التطبيق، المؤسسة المينائية.

Abstract

The objective of this study is to analyze the status of the application of the information security management system in accordance with international standards ISO 27001 in the port company of Skikda. To achieve the objectives of this study, we will rely on the descriptive analysis method, so we will use a questionnaire, on a random sample of 107 employees. In order to assess the compatibility of the enterprise information security management system with the requirements of ISO 27001 and to identify the strengths and weaknesses of the internal system applied in the enterprise.

The study found that the application rate of the system according to ISO 27001 at the enterprise level is 67.14%, the general trend was medium. In order to improve this rate, we recommend providing participants and business stakeholders with the skills necessary to develop the system, for the implementation of this standard (ISO 27001).

Keywords : information security; information security management system (ISMS) ; ISO 27001; requirements; the port company

* Auteur correspondant.

¹ University of 20 août 1955 skikda , Ecofima: Algeria, sab88mek@gmail.com.

² University of Constantine -2- Abelhamid Mehri, Réseau Maghtech: Algeria, mina.zerdoudi@hotmail.com.

Résumé :

L'objectif de cette étude est d'analyser l'état de lieux de l'application du système de management de la sécurité de l'information conformément aux normes internationales ISO 27001 dans l'entreprise portuaire de Skikda. Pour atteindre les objectifs de cette étude, nous nous appuyerons sur la méthode d'analyse descriptive, ainsi nous utiliserons un questionnaire, sur un échantillon aléatoire de 107 employés. Afin d'évaluer la compatibilité du système de management de la sécurité de l'information de l'entreprise aux exigences du système ISO 27001 et identifier les points forts et faibles du système interne appliqué dans l'entreprise.

L'étude a révélé que le taux d'application du système selon la norme ISO 27001 au niveau de l'entreprise est de 67,14%, la tendance générale était moyenne. Afin d'améliorer ce taux, nous recommandons de fournir aux participants et aux acteurs de l'entreprise les compétences nécessaires au développement du système, pour la mise en œuvre de cette norme (ISO 27001).

Mots clés : sécurité de l'information, système de management de la sécurité de l'information (SMSI), ISO 27001, exigences de l'application, entreprise portuaire.

Introduction

L'entreprise travaille dans un environnement dynamique caractérisé par la complexité et le changement en permanence, qui s'influence réciproquement, par conséquent elle obtient des diverses ressources des matières premières, des fonds, des travailleurs, de la technologie et des informations de cet environnement, tout en leur fournissant des différents marchandises, services et produits.

Comme l'énorme développement dans le domaine des médias automatisés et des technologies de l'information résultant de la révolution technique, et la forte croissance qui s'est produit dans les moyens de communication, les réseaux d'information et entrant dans l'ère de la mondialisation et d'Internet. L'émergence de nouveaux risques et menaces nationale et mondiale relatifs à la sécurité de l'information, qui nécessite de prendre tous les moyens disponibles et possibles pour la sécurité et la protection des systèmes de l'information, car il s'agit d'un ensemble de mesures préventives et de mesures utilisées pour se protéger contre les délits informatiques et Internet, et les menaces d'utilisation de technologies susceptibles d'affecter la confidentialité, l'intégrité ou la disponibilité des informations ou pouvant être associées à des appareils informatiques. Identique au vol ou à l'utilisation d'ordinateurs et de réseaux d'information comme médiateur dans la commission de délits.

C'est pourquoi l'Organisation internationale de normalisation ISO a développé une nouvelle série spécialisée dans la protection de l'information, qui est 2005 : 27001ISO, qui s'appelle les systèmes de management de la sécurité de l'information (exigences), car la norme ISO 27001 fournit à l'entreprise un modèle commun pour appliquer, exploiter et améliorer les systèmes de management de la sécurité de l'information.

Alors que les entreprises algériennes cherchent à mettre en place des systèmes d'information et à les gérer efficacement, l'Entreprise Portuaire de Skikda EPS est considérée parmi les entreprises algériennes auxquelles elle tient une grande importance en raison de sa possession d'une position stratégique importante dans les mouvements commerciaux.

- **La problématique de l'étude**

Dans le but d'analyser l'état de lieux de l'application du système de management de la sécurité de l'information dans l'Entreprise Portuaire de Skikda en Algérie avec le système de management de la sécurité de l'information selon les spécifications de la norme ISO 27001 en termes d'exigences de mise en œuvre du système. La question principale suivante a été posée :

Dans quelle mesure les exigences du système de management de la sécurité de l'information conformément à la norme internationale ISO 27001 à l'Entreprise Portuaire de Skikda sont-elles appliquées ?

Sous cette question principale, les sous-questions suivantes sont incluses :

- Dans quelle mesure l'exigence domaine du système de management de sécurité de l'information selon la norme internationale ISO 27001 est-elle appliquée ?
- Dans quelle mesure l'exigence des références normatives du système de management de sécurité de l'information selon la norme internationale ISO 27001 est-elle appliquée ?
- Dans quelle mesure dans l'exigence des termes et définitions du système de management de sécurité de l'information selon la norme internationale ISO 27001 est-elle appliquée ?
- Dans quelle mesure les exigences générales du système de management de sécurité de l'information selon la norme internationale ISO 27001 sont-elles appliquées ?
- Dans quelle mesure l'exigence de la responsabilité de la direction du système de management de sécurité de l'information selon la norme internationale ISO 27001 est-elle appliquée ?
- Dans quelle mesure l'exigence audits internes du système de management de sécurité de l'information selon la norme internationale ISO 27001 est-elle appliquée ?
- Dans quelle mesure l'exigence revue de la direction du système de management de sécurité de l'information selon la norme internationale ISO 27001 est-elle appliquée ?
- Dans quelle mesure l'exigence amélioration continue du système de management de sécurité de l'information selon la norme internationale ISO 27001 est-elle appliquée ?

- **Hypothèses de l'étude**

Sur la base de la question principale de l'étude et des sous-questions précédentes, et comme réponses initiales à celle-ci, les hypothèses suivantes ont été mises au point :

L'hypothèse principale :

Les exigences du système de management de la sécurité de l'information selon la norme internationale ISO 27001 à l'Entreprise Portuaire de Skikda ne sont pas appliquées au niveau de signification $0,05 \geq \alpha$.

Sous-hypothèses :

- L'exigence domaine du système de management de la sécurité de l'information selon la norme internationale ISO 27001 n'est pas appliquée au niveau de signification $0,05 \geq \alpha$.
- L'exigence des références normatives du système de management de la sécurité de l'information selon la norme internationale ISO 27001 n'est pas appliquée au niveau de signification $0,05 \geq \alpha$.
- L'exigence des termes et définitions pour le système de management de sécurité de l'information selon la norme internationale ISO 27001 n'est pas appliquée au niveau de signification $0,05 \geq \alpha$.
- Les exigences générales du système de management de la sécurité de l'information selon la norme internationale ISO 27001 ne sont pas appliquées au niveau de signification $0,05 \geq \alpha$.
- L'exigence de la responsabilité de la direction du système de management de sécurité de l'information selon la norme internationale ISO 27001 n'est pas appliquée au niveau de signification $0,05 \geq \alpha$.
- L'exigence audits internes du système de management de sécurité de l'information selon la norme internationale ISO 27001 n'est pas appliquée au niveau de signification $0,05 \geq \alpha$.

- L'exigence revue de la direction du système de management de la sécurité de l'information selon la norme internationale ISO 27001 n'est pas appliquée au niveau de signification $0,05 \geq \alpha$.
- L'exigence amélioration continue du système de management de sécurité de l'information selon la norme internationale ISO 27001 n'est pas appliquée au niveau de signification $0,05 \geq \alpha$.

En fonction de la réponse aux questions susmentionnées, nous pouvons connaître la disponibilité des exigences pour la mise en place d'un système de management de la sécurité de l'information compatible avec le système ISO 27001 dans l'Entreprise Portuaire de Skikda.

- **Objectifs de l'étude :**

L'étude vise à atteindre un ensemble d'objectifs, à savoir :

- Assurer des concepts modernes dans la qualité de la protection de l'information, en utilisant ISO27001 comme norme moderne pour la protection de l'information.
- Obtenir le maximum d'avantages de l'information efficacement.
- Clarifier le concept des dimensions du système de management de la sécurité de l'information.
- Connaître l'état de lieux du système de management de sécurité de l'information dans les entreprises économiques algériennes à travers l'Entreprise Portuaire de Skikda.

- **L'importance de l'étude :**

L'étude comprend la mise en œuvre des exigences du système de la sécurité d'information et la nécessité d'accorder une grande importance et de préserver les informations contre la falsification et le trafic, à cet égard, l'importance de l'étude se reflète en présentant aux entreprises le contenu de la norme ISO27001 comme un outil efficace qui accorde un certificat international selon lequel l'entreprise est soumise aux normes internationales en maintenant ses données et sa confidentialité.

Ce qui donne plus l'importance de l'étude, c'est que les résultats qui peuvent être atteints peuvent ouvrir de nouveaux horizons pour d'autres études prospectives, ce qui augmente l'importance de l'étude car il s'agit d'un nouveau sujet.

- **Études antérieures :**

A- Étude (NATACHA GONDRAN) intitulée :

"Système de diffusion d'information pour encourager les PME / PMI à améliorer leurs performances environnementales". Institut national des sciences appliquées de Lyon, France.

Il est indiqué dans cette étude que la plupart des petites et moyennes entreprises ne recherchent pas les informations environnementales de manière naturelle et spontanée, en raison du manque de capacités matérielles et humaines, et elle considère également l'environnement comme une contrainte qui entrave sa croissance et son développement.

L'objectif de l'étude étant de réaliser une analyse du système d'information environnementale pour les petites et moyennes entreprises afin d'y apporter des améliorations, dans le but d'aider et d'encourager ces entreprises à réduire les effets négatifs de l'environnement. L'étude était basée sur l'hypothèse que l'intégration des petites et moyennes entreprises dans leur environnement, ainsi que leur accès aux informations environnementales, il est nécessaire de contrôler ces effets négatifs mentionnés, et les résultats de l'étude ont montré que les petites et moyennes entreprises préfèrent s'appuyer sur le contact direct pour obtenir des informations, un diagnostic a été établi de la carence rencontrée par ces entreprises en matière d'informations environnementales.

B- Étude Muasher (2006).

Intitulée par : l'effet des facteurs organisationnels et techniques sur les applications des systèmes de gestion d'information (une étude appliquée dans le secteur bancaire jordanien).

L'étude visait à calculer l'effet des facteurs organisationnels et techniques sur les applications des systèmes de gestion d'information dans le secteur bancaire jordanien.

L'étude révèle qu'il existe un effet statistiquement significatif de la variable des facteurs techniques et des variables organisationnelles dans les applications des systèmes de gestion d'information, et l'étude a recommandé la nécessité d'impliquer les travailleurs et les employeurs dans le processus de conception et de développement des systèmes de l'information administrative.

C- Une étude de SUPATTRA BOONMAK (2007).

Intitulée par l'effet des systèmes d'information administrative et des systèmes d'information sur l'efficacité du travail administratif. L'étude a été établie pour mesurer l'influence des systèmes de gestion d'information et des technologies de l'information sur l'efficacité de la gestion de l'entreprise et sur sa stratégie commerciale.

L'étude a révélé à plusieurs résultats, dont le plus important est que les systèmes d'information administrative et les technologies de l'information augmentent l'efficacité de l'organisation et l'efficacité de ses performances et améliorent le travail son stratégique. Plus il était nécessaire de dépendre à la technologie de l'information, plus il était nécessaire de dépendre aux systèmes d'information administrative et de la technologie de l'information plus la productivité et l'efficacité de l'organisation seront augmenté plus la culture des travailleurs de l'entreprise vers l'efficacité et l'efficacité de la performance sera amélioré.

Notre étude menait à compléter les études précédentes sur le système d'information et les systèmes de sécurité de l'information de l'entreprise par des nouveaux points dans cette étude, à travers les conditions d'obtention du certificat ISO et de la norme ISO 27001 pour le système de management de la sécurité de l'information, en soulignant sa relation avec l'entreprise, et procéder des listes de contrôle et d'évaluation du système de sécurité de l'information.

1. PARTIE THEORIQUE : LA SECURITE DE L'INFORMATION

La partie théorique traite d'une approche générale de la sécurité de l'information et du système de gestion de la sécurité de l'information, en plus Iso 27001, et nous les aborderons à travers les éléments suivants :

1.1.la sécurité de l'information :

La sécurité de l'information fait partie des secteurs de sécurité sur lesquels s'appuient les organisations, dans cette composante, nous examinerons le concept de sécurité de l'information et son importance comme suite :

1.1.1 Définition de la sécurité de l'information

La sécurité de l'information est définie comme un ensemble de mesures préventives et de mesures utilisées dans le domaine technique ou préventif pour préserver les informations, le matériel et les logiciels, en plus des procédures liées à la préservation des travailleurs dans ce domaine (AL-Salami, 2000, p. 294).

Elle maintient la confidentialité, la disponibilité et l'intégrité des informations en tant qu'une origine dans les étapes de traitement, de conservation et de transfert, et cela est réalisé par l'application effective des politiques de sécurité à travers la sensibilisation, l'apprentissage et

la formation. La sécurité de l'information est basée sur un ensemble de procédures, de dispositions et de caractéristiques qui doivent être prises en considération pour préserver les informations, et par-dessus préserver les composants immatériels, les logiciels et le cadre humain, et la protection contre le piratage, l'espionnage, les polluants, le vol, la commutation, et les dommages intentionnels ou non intentionnels, ou l'accès sans autorisation. A ce titre, la norme ISO27001 est (AL-Danaf, 2013, p. 50).

La sécurité de l'information est basée sur des nombreuses dimensions dont la politique et l'organisation de la sécurité, la classification et le contrôle des actifs, ainsi que la sécurité individuelle afin de réduire les risques humains, les vols, les détournements de fonds ou l'utilisation abusive des installations, en outre, le contrôle d'accès (AL-hadeethi, 2001, p. 22), mais la politique de sécurité de l'information doit être claire, concise et spécifique. La logique de cet aspect est que la responsabilité impose une vérification de toutes les parties, et traite l'interaction entre les informations (Grand, 2000, p. 25), La sécurité de l'information vise également à protéger les intérêts ou les avantages de ces informations au profit de l'entreprise, ainsi qu'à protéger les systèmes de l'information et de la communication qui contribuent à fournir ces informations aux parties concernées et à les protéger de la faiblesse (Parker Xenia & autres, 2001, p. 12) .Pour atteindre l'objectif de sécurité de l'information, les données et les informations doivent être protégées contre toute modification non autorisée en spécifiant des pouvoirs dans le système de contrôle interne ou par la direction de l'entreprise (IIA, 2003, p. 3).

1.1.2 Définition de la sécurité de l'information :

L'importance de la sécurité de l'information consiste aux points suivants : (Farouk, 2008, p. 9).

- Les secteurs de la sécurité militaire et économique dépendent de l'exactitude et de la pertinence des informations.
- Les pays doivent disposer de mesures de sécurité viables couvrant les risques qui peuvent survenir en traitant avec d'autres parties.
- La nécessité croissante de créer un environnement électronique sécurisé au service des secteurs privé et public.
- La croissance rapide des utilisations des applications électroniques qui nécessitent un environnement sécurisé.
- La nécessité de protéger l'infrastructure du réseau de l'information afin de maintenir la continuité des activités.
- À mesure que la technologie de l'information se développe et prospère, des possibilités de cybercriminalité ont été disposées.

1-2 Définir le système de management de la sécurité d'information

Le système de gestion de la sécurité de l'information est basé sur des politiques et des procédures documentées qui sont adoptées et respectées et seront discutées comme suit :

1.2.1 Définition du certificat ISO 27001 :

Le certificat ISO 27001 est une norme internationale liée au système de management de la sécurité de l'information, et définit les exigences pour la mise en œuvre, le suivi et la révision, ISO

IEC27001, la maintenance, et l'amélioration du système de gestion, qui est un cadre de gestion et de contrôle intégré pour gérer les risques de sécurité de l'information de l'entreprise (comité des systèmes d'exploitation, 2010, p. 5). Il existe un ensemble de raisons qui poussent une entreprise à obtenir un certificat afin d'obtenir des avantages, de sorte qu'elle puisse différencier les concurrents et obtenir des instructions à faible coût, (Hinson, 2015, p. 20).

La norme ISO 27001 2013 : est un système de management de la sécurité de l'information qui est basé sur des politiques organisées, des processus approuvés et des procédures écrites qui sont adoptées, appliquées et respectées afin qu'elle soit accordée sous forme de certificats aux bénéficiaires pour assurer une sécurité adéquate de leurs informations et les protéger du piratage et de l'accès à celles-ci, puis les altérer, les saisir ou les détruire. et c'est en fait ce que prévoit la norme internationale ISO 27001 de la protection continue des informations en connaissant les actifs de l'organisation et en évaluant son importance sur la base des informations et des données qu'elle contient puis en connaissant et évaluant les risques attendus et en apportant les solutions appropriées pour les contenir, les traiter ou les corriger, qu'il s'agisse des solutions administratives, procédurales, techniques ou opérationnelles.

La norme internationale ISO27001 a été rendue en 2005 en tant que règle de pratique qui prend ses directives et sa tutelle de la norme internationale ISO17799 parallèlement à la norme britannique BS7799, et cela peut être considéré comme ISO27001 comme une base pour l'évaluation du système intégré de management de la protection de l'information (SMSI), ou c'est un document qui évalue tout système de la management de la protection de l'information (Calder&Watkins, 2008, p. 8)

Si l'entreprise souhaite développer et mettre en place un système de sécurité pour les systèmes de l'information et le maintenir, il faut éviter tout accès non autorisé aux ordinateurs, réseaux et données, en tenant compte du fait que le système est financièrement sécurisé, en construisant correctement le système et en formant les utilisateurs aux questions de sécurité(Alter, 1999).

1.2.2 Les avantages de son application :

La norme internationale mise à jour ISO 27001 2013 : est considérée comme l'une des spécifications de normes internationales distinctes si elle n'est pas la seule approuvée, car elle se caractérise par sa flexibilité en fonction de toutes les entreprise, secteurs et départements, qu'ils soient étatiques ou privés, de sorte que l'entreprise étudie les risques relatifs aux informations, les comprendre et les intégrer, puis construit un système de sécurité des informations cohérent qui réduit les risques potentiels et les catastrophes. C'est un système qui peut être développé, survécu et efficace. Il existe de nombreux avantages qui peuvent être réalisés. Nous mentionnons, par exemple, comme suit :

- La conformité avec les exigences réglementaires pour maintenir la sécurité et la confidentialité des données et des informations dans les secteurs étatiques et privés.
- Concevoir les meilleurs contrôles internes, les plus fiables et les moins chers correspondant à l'environnement de travail et au volume de l'activité.
- Promulguer une législation, établir des politiques et organiser les procédures basées sur l'évaluation des risques et développer les méthodes spécifiques pour faire face à ces risques attendus

1.2.3 Les Exigences ISO27001 :

ISO27001 est basée sur des exigences de base de sorte que ces exigences se composent de huit éléments et sont divisées en deux parties : dispositions générales et se composent du domaine dans lequel le domaine d'application et les références normatives sont clarifiés et qui clarifie la principale source d'application qui est ISO27001 : 2005, ISO17799 : 2005 pour l'application. En outre ces termes et définitions, pour clarifier les conditions d'application et la clarification des termes utilisés pour éviter la mauvaise compréhension des termes. Tandis que la deuxième section consiste aux principaux termes d'application de la norme et à la responsabilité de la direction afin qu'elle détermine la mesure de l'engagement de l'administration à appliquer les termes de la norme et à mobiliser toutes les ressources nécessaires pour le succès de l'application, ainsi que l'entraînement mental et les capacités de formation du personnel. Également l'audit interne du système de management de la sécurité de l'information, car l'entreprise effectue des contrôles internes à des intervalles pré-planifiés pour déterminer si le processus de demande est conforme aux plans mis en place, ainsi que pour détecter les écarts d'application. Sans oublier également la revue de la direction, et cela se fait à travers une révision des entrées et sorties du système, ainsi que l'amélioration du système, et ici l'amélioration continue du système est réalisée en définissant des mesures correctives, ainsi que des mesures préventives, pour éviter les erreurs (AL-Ali, 2009, pp. 60-61)

2. PARTIE PRATIQUE : L'ETUDE SUR TERRAIN

Afin de tester les hypothèses de l'étude et d'arriver à des résultats sur l'étendue de la conformité du système de gestion de la sécurité de l'information, l'établissement portuaire de skikda a été pris comme étude de cas.

2.1.Méthodologie de l'étude

Pour aborder le sujet d'étude, vous devez suivre les étapes suivantes :

2.1.1 Méthodes de traitement statistique :

Grâce au progiciel statistique de l'application des sciences sociales (spss), le traitement statistique a été effectué en analysant les données à l'aide des méthodes statistiques suivantes :

- Les statistiques descriptives représentées dans la mesure, les itérations et les pourcentages, en outre de la moyenne arithmétique et la déviation standards afin d'étudier les attitudes des individus de l'échantillon de l'étude à l'égard des variables de l'étude et de leur analyse.

- Le coefficient alpha de Cronbach pour mesurer la stabilité de l'outil d'étude.

- Utiliser le test simple T.

1.1.1. Choix de la population et l'échantillon de l'étude :

L'entreprise portuaire de SKIKDA a été choisie comme étude de cas, la population de l'étude a été estimée de 280 employés (différents cadres et agent de soutien), un échantillon aléatoire simple a été déterminée de 107 employés selon l'équation de Steven Thompson (Steven K Thompson, 2012, p51), 76 questionnaires ont été récupérés avec un taux de réponse de 71.02%.

2.2 Analyse des données de l'étude :

2.2.1 Pourcentage d'application selon likert échelle :

Tableau -1-: Évaluation selon Likert échelle pour adoption :

Champ	1	2	3
Moyenne arithmétique	1-1.66	1.67-2.34	2.35-3
Pourcentage	[33.33%-55.55% [	[55.55%-78% [	[78%-100%]

Source : par le chercheur à base des résultats de l'SPSS.

2.2.2 La stabilité du questionnaire de l'étude :

Pour étudier la cohérence interne de différents axes du questionnaire, nous avons calculé l'indice alpha de Cronbach, comme indique le tableau suivant :

Tableau -2 -: Les indices de stabilités (Alpha Cronbach) :

Axes	Phrases	Indice alpha cronbach
Domaine	1-02	0.828
Références normatives	03-07	0.905
Termes et définitions	08-12	0.786
Exigences générales	13-15	0.716
Responsabilité de la direction	16-18	0.746
Audit interne	19-24	0.757
Revue de la direction	25-28	0.699
Amélioration du système	29-34	0.695
Total	1-34	0.953

Source : par le chercheur à base des résultats de l'SPSS.

Selon les résultats du tableau, la valeur d'alpha Cronbach pour les différents axes est supérieure à 60%, les valeurs sont entre 0.695 et 0.905 (élevés), par ailleurs la valeur globale du coefficient d'alpha Cronbach est de 0.953, qui présentent une valeur élevée, cela signifie la stabilité et la cohérence de différents axes du questionnaire.

Cela signifie que l'outil de l'étude est stable et précis, pour cela nous sommes confiant de la validité du questionnaire et sa pertinence pour analyser les résultats, répondre aux questions de l'étude et tester les hypothèses.

2.3 Les résultats de l'étude :

Nous pouvons résumer les différentes phrases des axes des exigences du système de la gestion de la sécurité de l'information dans le tableau suivant :

Tableau -3 -: Résultats des réponses de l'échantillon de l'étude sur les exigences du système de la gestion de la sécurité de l'information

N° axe	Axe	Moyenne arithmétique	Déviati on standard	Cla ssement	Évaluation
1	Domaine	2.25	0,45550	5	Partiellement appliqué
2	Références normatives	2.40	0,40890	3	Appliqué
3	Termes et définitions	1,2498	0,50200	8	Non appliqué
4	Exigences générales	2,4999	0,45109	2	Appliqué
5	Responsabilité de la direction	1.9998	0,41658	7	Partiellement appliqué
6	Audits internes	2.25	0,39039	4	Partiellement appliqué
7	Revue de la direction	2,625	0,49004	1	Appliqué
8	Amélioration du système	1,5998	0,35439	6	Non appliqué
TOTAL	Exigences du système	2,0142	0,39889	/	Partiellement appliqué

Source : par le chercheur à base des résultats de l'SPSS.

- La moyenne globale du premier axe est de 2.25 avec une déviation standard de 0.4550, ce qui indique une application partielle pour l'exigence domaine du système de management de la sécurité de l'information selon l'échantillon de l'étude.
- La moyenne globale du deuxième axe est de 2.40 avec une déviation standard de 0.40890, ce qui indique une application totale pour l'exigence référence normatives du système de management de la sécurité de l'information selon l'échantillon de l'étude.
- La moyenne globale du troisième axe est de 1.2498 avec une déviation standard de 0.50200, ce qui indique que l'exigence Termes et définitions du système de management de la sécurité de l'information est non appliquée selon l'échantillon de l'étude.
- La moyenne globale du quatrième axe est de 2.4999 avec une déviation standard de 0.45109, ce qui indique une application totale pour l'Exigences générales du système de management de la sécurité de l'information selon l'échantillon de l'étude.
- La moyenne globale du cinquième axe est de 1.9998 avec une déviation standard de 0.41658, ce qui indique une application partielle pour l'exigence Responsabilité de direction du système de management de la sécurité de l'information selon l'échantillon de l'étude.
- La moyenne globale du sixième axe est de 2.25 avec une déviation standard de 0.39039, ce qui indique une application partielle l'exigence Audit interne du système de management de la sécurité de l'information selon l'échantillon de l'étude.
- La moyenne globale du septième axe est de 2.625 avec une déviation standard de 0.49004, ce qui indique une application totale pour l'exigence revue de la direction du système de management de la sécurité de l'information selon l'échantillon de l'étude.

- La moyenne globale du huitième axe est de 1.5998 avec une déviation standard de 0.35439, ce qui indique que l'exigence amélioration du système du système de management de la sécurité de l'information est non appliquée selon l'échantillon de l'étude.
- En dernier la moyenne globale est de 2.0142 avec une déviation standard de 0.39889, ce qui indique une application partielle aux différentes exigences du système de management de la sécurité de l'information dans l'entreprise portuaire de SKIKDA selon l'échantillon de l'étude.
- **Tester les hypothèses de l'étude :**
 - **Teste de sous- l'hypothèse 1 :**

L'exigence domaine, du système de management de la sécurité de l'information selon la norme internationale ISO 27001 n'est pas appliquée au niveau de l'entreprise portuaire SKIKDA.

Tableau -4 -: Test T et niveau de signification pour mesurer l'application de l'exigence domaine du système de management de la sécurité de l'information au niveau de l'entreprise portuaire SKIKDA.

Dimension	Moyenne arithmétique	Déviation standard	Taux d'application	Valeur T	Signification
domaine	2.25	0.45550	75%	7.522	0.000

Source : par le chercheur à base des résultats de l'SPSS.

Le tableau N°4 représente le niveau d'application de l'exigence domaine du système de management de la sécurité de l'information au niveau de l'entreprise portuaire de SKIKDA.

les résultats montrent que la moyenne arithmétique est de 2.25 et la déviation standard est de 0.45550, avec un taux moyen d'application de 75% de l'exigence domaine selon les personnes de l'échantillon de l'étude, aussi la valeur de T calculée est de 7.522, ce qui est supérieur à la valeur de T tabulaire de 2.66, avec un niveau significatif 0.000 qui est inférieur à 0.05.

Pour cela nous refusons l'hypothèse H0, et nous acceptons l'hypothèse alternative qui suppose que : L'exigence domaine, du système de management de la sécurité de l'information selon la norme internationale ISO 27001 est appliquée au niveau de l'entreprise portuaire SKIKDA.

Cependant, cette exigence à des points faible, mais partielle ce sont :

- L'entreprise dispose d'un guide sur le système de la gestion de la sécurité de l'information, mais il n'est pas mis en mise à jour.
- le manque d'intérêt et de la culture sur le système de la gestion de la sécurité de l'information chez les employés de l'entreprise.

- **Teste de sous- l'hypothèse 2 :**

L'exigence référence normative, du système de management de la sécurité de l'information selon la norme internationale ISO 27001 n'est pas appliquée au niveau de l'entreprise portuaire SKIKDA.

Tableau -5 -: Test T et niveau de signification pour mesurer l'application de l'exigence référence normative du système de management de la sécurité de l'information au niveau de l'entreprise portuaire SKIKDA.

Dimension	Moyenne arithmétique	Déviation standard	Taux d'application	Valeur T	signification
Références normatives	2.40	0.40890	80%	9.061	0.000

Source : par le chercheur à base des résultats de l'SPSS.

Le tableau N°5 représente le niveau d'application de l'exigence référence normative, du système de management de la sécurité de l'information au niveau de l'entreprise portuaire de SKIKDA.

Les résultats montrent que la moyenne arithmétique est de 2.40 et la déviation standard est de 0.40890, avec un taux élevé d'application de 80% de l'exigence référence normative selon les personnes de l'échantillon de l'étude, aussi la valeur de T calculée est de 9.061, ce qui est supérieur à la valeur de T tabulaire de 2.66, avec un niveau significatif 0.000 qui est inférieur à 0.05.

Pour cela nous refusons l'hypothèse H0, et nous acceptons l'hypothèse alternative qui suppose que : L'exigence référence normative, du système de management de la sécurité de l'information selon la norme internationale ISO 27001 est appliquée au niveau de l'entreprise portuaire SKIKDA.

On peut constater quelques points faibles dans l'entreprise portuaire de SKIKDA tel que l'entreprise ne maintienne pas et surveille pas son système de la gestion de la sécurité de l'information.

- **Teste de sous- l'hypothèse 3 :**

L'exigence termes et définitions, du système de management de la sécurité de l'information selon la norme internationale ISO 27001 n'est pas appliquée au niveau de l'entreprise portuaire SKIKDA.

Tableau -6 -: Test T et niveau de signification pour mesurer l'application de l'exigence termes et définitions du système de management de la sécurité de l'information au niveau de l'entreprise portuaire SKIKDA.

Dimension	Moyenne arithmétique	Déviations standard	Taux d'application	Valeur T	Signification
Termes et définitions	1.2498	0.50200	41.66%	1.78	0.07

Source : par le chercheur à base des résultats de l'SPSS.

Le tableau N°6 représente le niveau d'application de l'exigence termes et définitions, du système de management de la sécurité de l'information au niveau de l'entreprise portuaire de SKIKDA.

Les résultats montrent que la moyenne arithmétique est de 1.2498 et la déviation standard est de 0.50200, avec un taux faible d'application de 41.66% de l'exigence termes et définitions selon les personnes de l'échantillon de l'étude, aussi la valeur de T calculée est de 1.78, ce qui est inférieur à la valeur de T tabulaire de 2.66, avec un niveau significatif 0.07 qui est supérieur à 0.05.

Pour cela nous acceptons l'hypothèse H0, qui suppose que : L'exigence termes et définitions, du système de management de la sécurité de l'information selon la norme internationale ISO 27001 n'est pas appliquée au niveau de l'entreprise portuaire SKIKDA.

On peut expliquer ce faible taux d'application dans les points suivants :

- l'amélioration continue du système de management de la sécurité de l'information est quasiment absente au sein de l'entreprise portuaire de SKIKDA.
- les exigences de contrôle de la protection des informations sont non exercées au sein de l'entreprise portuaire de SKIKDA.
- l'entreprise ne dispose pas de moyens, de techniques ou de systèmes suffisants pour contrôler la protection de ses informations.
- l'entreprise ne dispose pas d'un guide qui peut expliquer les différentes modalités du système de gestion de la sécurité de l'information.

Teste de sous- l'hypothèse 4 :

Les exigences générales, du système de management de la sécurité de l'information selon la norme internationale ISO 27001 n'est pas appliquée au niveau de l'entreprise portuaire SKIKDA.

- **Teste de sous- l'hypothèse 4 :**

Tableau -7 -: Test T et niveau de signification pour mesurer l'application des exigence générales du système de management de la sécurité de l'information au niveau de l'entreprise portuaire SKIKDA.

Dimension	Moyenne arithmétique	Déviati on standard	Taux d'application	Valeur T	signification
Exigences générales	2.4999	0.45109	83.33%	8.943	0.000

Source : par le chercheur à base des résultats de l'SPSS.

Le tableau N°7 représente le niveau d'application des exigences générales, du système de management de la sécurité de l'information au niveau de l'entreprise portuaire de SKIKDA.

Les résultats montrent que la moyenne arithmétique est de 2.4999 et la déviation standard est de 0.45109, avec un taux élevé d'application de 83.33% des exigences générales selon les personnes de l'échantillon de l'étude, aussi la valeur de T calculée est de 8.943, ce qui est supérieur à la valeur de T tabulaire de 2.66, avec un niveau significatif 0.000 qui est inférieur à 0.05.

Pour cela nous refusons l'hypothèse H0, et nous acceptons l'hypothèse alternative qui suppose que : les exigences générales, du système de management de la sécurité de l'information selon la norme internationale ISO 27001 est appliquée au niveau de l'entreprise portuaire SKIKDA.

Mais on constate comme même, que l'entreprise ne considère pas le système management de la sécurité de l'information dans l'amélioration continue du système de documentation et la gestion de l'information.

- **Teste de sous- l'hypothèse 5 :**

L'exigence responsabilité de la direction, du système de management de la sécurité de l'information selon la norme internationale ISO 27001 n'est pas appliquée au niveau de l'entreprise portuaire SKIKDA.

Tableau -8 -: Test T et niveau de signification pour mesurer l'application de l'exigence responsabilité de la direction du système de management de la sécurité de l'information au niveau de l'entreprise portuaire SKIKDA.

Dimension	Moyenne arithmétique	Déviati on standard	Taux d'application	Valeur T	signification
Responsabilité de la direction	1.9998	0.41658	66.66%	10.975	0.000

Source : par le chercheur à base des résultats de l'SPSS.

Le tableau N°8 représente le niveau d'application de l'exigence responsabilité de la direction, du système de management de la sécurité de l'information au niveau de l'entreprise portuaire de SKIKDA.

Les résultats montrent que la moyenne arithmétique est de 1.9998 et la déviation standard est de 0.41658, avec un taux élevé d'application de 66.66% de l'exigence responsabilité de la direction selon les personnes de l'échantillon de l'étude, aussi la valeur de T calculée est de 10.975, ce qui est supérieur à la valeur de T tabulaire de 2.66, avec un niveau significatif 0.000 qui est inférieur à 0.05.

Pour cela nous refusons l'hypothèse H_0 , et nous acceptons l'hypothèse alternative qui suppose que : L'exigence responsabilité de la direction, du système de management de la sécurité de l'information selon la norme internationale ISO 27001 est appliquée au niveau de l'entreprise portuaire SKIKDA.

On peut citer quelques points faibles comme :

- l'entreprise ne maintient pas la mise en œuvre des dispositions du système de management de la sécurité de l'information par l'administration.
- L'administration utilise toutes les ressources nécessaires pour mener à bien ses responsabilités, mais de manière irrationnelle.
- L'administration assure la formation mentale et la formation des capacités de l'équipe, mais ces formations son non organisées.

• **Teste de sous- l'hypothèse 6 :**

L'exigence audit interne, du système de management de la sécurité de l'information selon la norme internationale ISO 27001 n'est pas appliquée au niveau de l'entreprise portuaire SKIKDA.

Tableau -9 -: Test T et niveau de signification pour mesurer l'application de l'exigence audit interne du système de management de la sécurité de l'information au niveau de l'entreprise portuaire SKIKDA.

Dimension	Moyenne arithmétique	Déviati on standard	Taux d'application	Valeur T	signification
Audit interne	2.25	0.39039	75%	10.891	0.000

Source : par le chercheur à base des résultats de l'SPSS.

Le tableau N°9 représente le niveau d'application de l'exigence audit interne, du système de management de la sécurité de l'information au niveau de l'entreprise portuaire de SKIKDA.

Les résultats montrent que la moyenne arithmétique est de 2.25 et la déviation standard est de 0.39039, avec un taux élevé d'application de 75% de l'exigence audit interne selon les personnes de l'échantillon de l'étude, aussi la valeur de T calculée est de 10.891, ce qui est supérieur à la valeur de T tabulaire de 2.66, avec un niveau significatif 0.000 qui est inférieur à 0.05.

Pour cela nous refusons l'hypothèse H_0 , et nous acceptons l'hypothèse alternative qui suppose que : L'exigence audit interne, du système de management de la sécurité de l'information selon la norme internationale ISO 27001 est appliquée au niveau de l'entreprise portuaire SKIKDA.

On peut détecter quelques points faibles :

- l'entreprise n'effectue pas une vérification interne à des intervalles préétablis pour déterminer si la mise en œuvre de la sécurité de l'information est conforme aux plans mise en place.
- La direction de l'entreprise demande aux auditeurs internes d'utiliser des outils technologiques avancés pour la sécurité et la confidentialité de ses informations, mais ces outils ne sont pas disponibles en quantité et en qualité.

• **Teste de sous- l'hypothèse 7 :**

L'exigence revue de la direction, du système de management de la sécurité de l'information selon la norme internationale ISO 27001 n'est pas appliquée au niveau de l'entreprise portuaire SKIKDA.

Tableau -10 -: Test T et niveau de signification pour mesurer l'application de l'exigence revue de la direction du système de management de la sécurité de l'information au niveau de l'entreprise portuaire SKIKDA.

Dimension	Moyenne arithmétique	Déviati on standard	Taux d'application	Valeur T	signification
Revue de la direction	2.625	0.49004	87.50%	10.801	0.000

Source : par le chercheur à base des résultats de l'SPSS.

Le tableau N°10 représente le niveau d'application de l'exigence revue de la direction, du système de management de la sécurité de l'information au niveau de l'entreprise portuaire de SKIKDA.

Les résultats montrent que la moyenne arithmétique est de 2.625 et la déviation standard est de 0.49004, avec un taux élevé d'application de 87.50% de l'exigence revue de la direction selon les personnes de l'échantillon de l'étude, aussi la valeur de T calculée est de 10.801, ce qui est supérieur à la valeur de T tabulaire de 2.66, avec un niveau significatif 0.000 qui est inférieur à 0.05.

Pour cela nous refusons l'hypothèse H0, et nous acceptons l'hypothèse alternative qui suppose que : L'exigence revue de la direction, du système de management de la sécurité de l'information selon la norme internationale ISO 27001 est appliquée au niveau de l'entreprise portuaire SKIKDA.

On peut citer quelques points faibles comme :

- l'entreprise examine les lois et les législations de l'État en matière de protection et sécurité de l'information, mais elle ne les applique pas immédiatement.

- **Teste de sous- l'hypothèse 8 :**

L'exigence amélioration continue, du système de management de la sécurité de l'information selon la norme internationale ISO 27001 n'est pas appliquée au niveau de l'entreprise portuaire SKIKDA.

Tableau -11 -: Test T et niveau de signification pour mesurer l'application de l'exigence amélioration continue du système de management de la sécurité de l'information au niveau de l'entreprise portuaire SKIKDA.

Dimension	Moyenne arithmétique	Déviati on standard	Taux d'application	Valeur T	signification
Amélioration continue	1.5998	0.35439	53.32%	1.891	0.06

Source : par le chercheur à base des résultats de l'SPSS.

Les résultats montrent que la moyenne arithmétique est de 1.5998 et la déviation standard est de 0.35439, avec un taux faible d'application de 53.32% de l'exigence amélioration continue selon les personnes de l'échantillon de l'étude, aussi la valeur de T calculée est de 1.891, ce qui est inférieur à la valeur de T tabulaire de 2.66, avec un niveau significatif 0.06 qui est supérieur à 0.05.

Pour cela nous acceptons l'hypothèse H0, qui suppose que : L'exigence amélioration continue, du système de management de la sécurité de l'information selon la norme internationale ISO 27001 n'est pas appliquée au niveau de l'entreprise portuaire SKIKDA.

On peut expliquer ce faible taux d'application dans les points suivants :

- l'entreprise ne considère pas le système de management de sécurité de l'information comme une sorte d'amélioration continue du système de documentation et de gestion de l'information.
- Le système de sécurité de l'information ne fournit pas aux participants les compétences nécessaires pour effectuer des revues internes sur les systèmes de management de la sécurité de l'information.

• **Teste de l'hypothèse principale :**

Les exigences du système de management de la sécurité de l'information selon la norme internationale ISO 27001 n'est pas appliquée au niveau de l'entreprise portuaire SKIKDA.

Tableau -12 -: Test T et niveau de signification pour mesurer l'application des exigences du système de la gestion de la sécurité de l'information au niveau de l'entreprise portuaire SKIKDA.

Dimension	Moyenne arithmétique	Déviati on standard	Taux d'application	Valeur T	signification
Exigences du système	2.0142	0.39889	67.14%	10.871	0.000

Source : par le chercheur à base des résultats de l'SPSS.

Les résultats montrent que la moyenne arithmétique est de 2.0142 et la déviation standard est de 0.39889, avec un taux élevé d'application de 67.14% des exigences du système de management de la sécurité de l'information selon les personnes de l'échantillon de l'étude, aussi la valeur de T calculée est de 10.871, ce qui est supérieur à la valeur de T tabulaire de 2.66, avec un niveau significatif 0.000 qui est inférieur à 0.05.

Pour cela nous refusons l'hypothèse H0, et nous acceptons l'hypothèse alternative qui suppose que : Les exigences du système de management de la sécurité de l'information selon la norme internationale ISO 27001 est appliquée au niveau de l'entreprise portuaire SKIKDA.

L'entreprise doit assurer une amélioration continue des différentes activités de l'entreprise afin de pouvoir répondre aux exigences de la mise en œuvre d'un système de management de la sécurité de l'information ISO27001 et bénéficier des avantages.

Conclusion :

Après avoir étudié les points forts et faibles de l'application des exigences du système de management de la sécurité de l'information au sein de l'entreprise portuaire de SKIKDA, dont le taux de conformité avec les exigences du SMSI est de 67.14%, ce qui représente un taux de conformité moyen. Cette conformité moyenne est due au taux élevé d'application des exigences références normatives, exigences générales, exigences audits internes et revue de direction du SMSI, aussi un taux d'application moyen d'exigences domaine et exigence responsabilité de la direction.

Sans oublier le déséquilibre enregistré dans les exigences de termes et définitions et l'exigence de l'amélioration continue du SMSI au sein de l'entreprise portuaire SKIKDA.

Pour cela, nous suggérons les recommandations suivantes :

- l'entreprise doit obtenir un certificat d'ISO 27001 (système de management de la sécurité de l'information)

- l'entreprise doit assurer que le personnel est sensibilisé à la politique de sécurité de l'information et conscient de sa contribution à l'efficacité du SMSI.
- Sensibiliser le personnel aux différents termes du système de management de la sécurité de l'information en créant un guide.
- fournir un guide du système de management de la sécurité de l'information pour sensibiliser les clients de l'entreprise et les parties prenantes.
- réaliser des formations pour le personnel de l'entreprise par des personnes qualifiées et expérimentés.
- Les audits internes sont planifiés, établis et mis en œuvre à des intervalles déterminés pour assurer la réalisation des plans de l'entreprise.
- l'entreprise doit documenter ces buts et ces objectifs sociaux, environnementaux, technologiques et économiques...
- l'entreprise doit utiliser des outils technologiques avancés pour la sécurité et la confidentialité de ces informations.
- l'entreprise doit mettre en œuvre les différents lois et législatifs relatives au système de management de la sécurité de l'information.
- l'entreprise doit adopter un système de management de la sécurité de l'information pour fournir aux participants les compétences nécessaires pour assurer des audits internes des systèmes de management de la sécurité de l'information et contribuer à l'amélioration continue.
- La nécessité d'une reconnaissance claire du système de management de la sécurité de l'information conformément à la norme ISO 27001.
- Déterminer le domaine d'intérêt des parties prenantes et les impliquer dans la prise de décisions de l'entreprise.
- Construire un réseau de communication spécialisé dans l'information administrative et sociale au sein de l'entreprise, lié à son environnement externe.
- L'entreprise doit créer des initiatives volontaires.
- La nécessité d'avoir un guide pour la mise en œuvre d'un système de management de la sécurité de l'information au sein de l'entreprise
- L'entreprise doit mettre en service un personnel expérimenté et compétent pour expliquer, enseigner et généraliser le système de management de la sécurité de l'information.
- L'Institut national de normalisation doit redoubler d'efforts pour définir les besoins nationaux dans le domaine de la normalisation, notamment la norme internationale de la sécurité et la protection de l'information, assurer la mise en œuvre d'un programme national de normalisation et assurer la diffusion des informations relatives à la normalisation.
- Les normes mondiales de la sécurité de l'information disponibles ne peuvent être exploitées que si elles sont correctement mises en œuvre avec la participation de toutes les parties à tous les niveaux de l'entreprise.
- Les entreprises algériennes doivent avoir un lien réaliste entre la gestion du cycle de vie de l'information et la norme ISO 27001, car ce lien fournira des moyens efficaces et performants pour traiter l'information, aussi obtenir des certificats ISO dans ce domaine permettra de gagner un avantage concurrentiel et une place mondiale.

- La norme internationale ISO 27001 est considérée comme l'une des normes internationales distinguées, qui se caractérise par sa flexibilité, afin d'être compatible avec toutes les entreprises étatiques ou privées, lors l'entreprise étudiera les risques liés à ses informations et à sa compréhension, puis construira un système de la sécurité de l'information qui diminuera les risques et qui pourra développer une méthodologie Clair définie.

- le système de management de la sécurité de l'information doit être documenté, publié et autorisé à tout le personnel de l'entreprise.

Bibliographie

- 1-AL-Ali, A. s. (2009). *département des projets généraux, maison AL-Masirah pour l'édition et la distribution.*
- 2-AL-Danaf, A. m. (2013). *état de lieux su système de management de la sécurité de l'information dans les gacultés technique du secteur de gaza et les moyens du développement du SMSI, Magister en management, université islamique à gaza, faculté de commerce.*
- 3-AL-hadeethi, y. (2001). *ph-d,uk, post doc MBI,berlin industrial optical communication systems security and disaster management alternatives dept of physics, faculty of science king abdul aziz university kingdom of saudi arabia, jaddah 21589, p.o box80203.*
- 4-AL-Salami, A. A.-R. (2000). *Technologie de l'information, 3eme édition, jordanie, dar Al-Bahaa pour l'édition et la distribution.*
- 5-Alter, S. (1999). *information system: A management perspective, third editio-wesley publisher INC New york.*
- 6-Calder, A., & Watkins, s. (2008). *IT governance amanager's guide to data security and ISO27001/ ISO27002, quatrième édition, London and philadelphia, british.*
- comité des systèmes d'exploitation, d. n. (2010). *Introduction aux politiques et normes de sécurité de l'information, Ministère de la présidence du conseil des ministres, centre national d'information, département technique de la qualité et du qualité et du développement- unité des normes, premiers numér.*
- 7-Farouk, F. H. (2008). *Une introduction à la sécurité de liinformation et à la définition de la criminalié électronique...Ministère de l'intérieur/ direction des technologiede l'information / département de la formation et du développement/ division des études et de la recherch.*
- 8-Grand, c. (2000). *ozier, will information, security management element, audit and control IIA, vol8, March.*
- 9-Hinson, G. (2015). *Iso 27001 security: the financial implication of implementing iso IEC 27001 and 27002 a generic cost benefit model, isect, LTD.*
- 10-IIA. (2003). *managing security information risk management, IT Auditor, march.*
- 11-Parker Xenia, l., & autres. (2001). *information sicurity governance, audit and control, vol4, february15.*
- 12-Qasim Nayef, A. (2005). *Département de la qualité totale et des réclamations iso 2000: 9001, première édition, dar Al thaqafa pour l'édition et la distribution Amman, jordanie.*