Le contrôle interne : dispositif permanent et indispensable pour la maitrise des risques liées aux systèmes d'information

Internal control : a permanent and essential system for controlling risks related to information systems

BOUYAHIAOUI Adel [1], DAHIA Abdelhafidh [2]

[1] Doctorant à l'école supérieure de commerce -Kolea, a_bouyahiaoui@esc-alger.dz ,

[2] Professeur à l'école supérieure de commerce -Kolea, a_dahia@esc-alger.dz ,

Reçu le: 17/07/2022 Accepté le:04/10/2022 Publié le: 31/10/2022

Abstract: the appearence of many global financial contempts led to an increased interest on the related aspects as internal control and safe information. In a digital environment, an internal control framework for mastering the risks linked to IS is highly needed.

A study had been carried out to insure the efficiency of the internal control in the mastery of risks related to IS near 27 algerian companies represented by 56 employees.

As a test for the study hypothesies, individual-sample tests had been performed at α = 5 % Results showed that the internal control system of safe information had a very important role in the prevention of IS risks.

Key-words: internal control system, safe information, IS risks, COSO, COBIT.

Jel Classification codes: *C42, C52, C87, M42, L86.*

Résumé: Après l'apparition de nombreux scandales financiers mondiaux, l'importance des questions connexes telles que le contrôle interne et la sécurité de l'information ont considérablement augmenté. Un cadre de contrôle interne pour la maitrise des risques liées aux SI est devenu indispensable dans un environnement caractérisé par le numérique.

Une étude de cas a été menée pour vérifier le rôle du dispositif du contrôle interne dans la maitrise des risques liés aux systèmes d'information. Cette étude a été faite à l'aide d'une enquête de perception auprès d'une 27 entreprise algérienne représentée par 56 individus.

Afin de tester les hypothèses de l'étude, des tests à échantillon unique ont été réalisés à α = 5%. Les résultats montrent que le dispositif du contrôle interne des systèmes d'information joue un rôle très important dans la prévention des risques liées aux SI.

Mots clés : Système d'information, contrôle interne, contrôle interne des SI, COSO, COBIT.

Codes de classification JEL : **C42 ; C52 ; C87 ; M42 ; L86**.

Auteur correspondant *: BOUYAHIAOUI Adel,* ***Email*** *: a_bouyahiaoui@esc-alger.dz*

Le titre de l'article : Le contrôle interne : dispositif permanent et indispensable pour la maitrise des risques liées aux systèmes d'information

1-Introduction

Le système d'information est devenu la colonne vertébrale d'une entreprise ou d'une administration moderne, dont il irrigue toutes les fonctions pour contribuer à la fois à leur efficacité opérationnelle et à leur transformation stratégique. Il est donc au cœur de tous les métiers, et embarque les éléments de standardisation, les besoins de spécificités et, les contrôles de sécurité et de performance. Dans une économie globalisée avec des processus de plus en plus complexes, il est devenu le garant de facto de la protection de l'information, de la sincérité des opérations, de la vitesse d'exécution et donc de l'excellence opérationnelle. Et, de simple pourvoyeur de systèmes et de technologies, la Direction des systèmes d'information a vu son rôle évoluer vers leur utilisation optimale par les métiers et les utilisateurs au service de la performance de l'entreprise.

Compte tenu de son rôle, la pertinence du contrôle interne du système d'information, c'est-à-dire sa bonne maîtrise, est un élément clé de succès des organisations. Rappelons que, selon le cadre de référence de l'AMF, un bon contrôle interne contribue à la maîtrise des activités d'une organisation, à l'efficacité de ses opérations, à l'utilisation efficiente de ses ressources, et doit lui permettre de prendre en compte de manière appropriée les risques significatifs. Le contrôle interne des systèmes d'information est donc un sujet prioritaire pour une organisation, et encore plus actuellement où l'économie mondiale subit une crise d'une rare intensité.

Le contrôle des SI se matérialise par des dispositifs de contrôle interne qui définissent les règles et procédures à suivre et l'évaluation de l'actif immatériel de l'informatique et la fiabilité des informations financière (David & Valérié, 2013).

À l'ère du numérique, l'absence d'un dispositif du contrôle des systèmes d'information dans une certaine entreprise implique que l'ensemble de l'entreprise est construit sur une base fragile telle qu'elle ne peut survivre à aucun test de contrôle interne connexe, des nouveaux risques sont nées tels que : les fuites d'information, destruction des donnés, banalisation de l'accès aux SI …etc. (J.C & L.E, 2002)

Les systèmes d'information dans les entreprises nécessitent de nombreux contrôles internes en raison de la mise en œuvre généralisée de l'informatique et de la nécessité de minimiser les problèmes.

Étant donné que les types du contrôle actuellement utilisés ne peuvent pas réglementer efficacement ou complètement la robustesse d'un cadre de contrôle interne, en particulier lorsqu'il est incorporé dans les systèmes d'information actuels, de nombreuses institutions ont établi leurs propres ensembles de critères de sécurité de l'information.

Une série de normes et de critères ont été élaborés tels que les objectifs de contrôle pour les technologies de l'information et connexes (COBIT). COBIT complète le cadre d'entreprise COSO en termes d'évaluation du contrôle interne

et de l'équilibre des risques dans les environnements à forte intensité informatique ((ITGI), 2005)

Le système d'information, objet et moyen du contrôle interne de l'entreprise, est donc un sujet majeur sur lequel nous allons soulever la problématique suivante:

Comment le dispositif du contrôle interne peut prévenir dans les risques liés aux SI ?

Afin de répondre au problème, nous avons développé les hypothèses suivantes :

H1 : Le contrôle interne des systèmes d'information contribue à prévenir les risques des SI à travers la conformité aux instructions de la direction générale, aux lois et règlements ;

H2 : Le contrôle interne des systèmes d'information contribue à prévenir les risques des SI à travers l'utilisation optimale des ressources affectées et la maîtrise des processus ;

H3 : Le contrôle interne des systèmes d'information contribue à prévenir les risques des SI à travers l'identification, l'analyse et l'évaluation des risques ;

H4 : Le contrôle interne des systèmes d'information contribue à prévenir les risques des SI à travers la sécurité des actifs et la protection des données ;

H5 : Le contrôle interne des systèmes d'information contribue à prévenir les risques des SI à travers l'amélioration de la qualité de l'information financière, opérationnelle et de gestion.

Les études précédentes :

La recherche d'études antérieures liées au sujet de notre étude a montré que la plupart d'entre elles sont encore au stade de définition et d'exploration en raison de la nature de la technologie d'information, sa modernité, et le manque de recherche académique dont elle a traité, notamment en Algérie, et cette étude est considérée comme une pierre angulaire pour ouvrir la porte à la recherche sur ce sujet précieux et intéressant afin de montrer l'importance du contrôle interne dans la maitrise des risques liées aux systèmes d'information, parmi les études précédentes qui ont été faites :

- Etude descriptive de Jing Fan Pengzhu Zhang David C. Yen (2013), intitulée Internal Control Framework of a Compliant ERP System, l'objectif de Cette étude tente d'établir de bons standards de contrôle interne pour les ERP afin de réussir la performance du SI.
- Etude descriptive de Djekidel Yahia , Messaoudi Abdelhadi, Boujlal Ahmed (2020), intitulée Le contrôle interne en milieu informatique , L'objectif de cette étude est d'appréhender le dispositif de contrôle interne ainsi que d'apprécier sa capacité à gérer les risques en milieu informatique, l'étude a conclu que la mise en place de dispositif de contrôle interne repose en grande partie sur le contrôle de l'informatique.

Le titre de l'article : Le contrôle interne : dispositif permanent et indispensable pour la maitrise des risques liées aux systèmes d'information

1- le contrôle interne dans un environnement informatique:

Le terme contrôle interne faisait partie du vocabulaire des entreprises depuis de nombreuses années, mais il n'a jamais eu de définition précise et cohérente historiquement. COSO développé une définition qui précise que le contrôle interne est un dispositif de la société qui contribue à la maîtrise de ses activités, à l'efficacité de ses opérations et à l'utilisation efficiente de ses ressources (IFACI, Le dispositif du controle interne: cadre de référence, 2007).
Le contrôle interne est un processus qui est affecté par le conseil d'administration d'une entité, la direction et les autres membres du personnel, conçus pour fournir une assurance raisonnable en ce qui concerne la réalisation des objectifs de l'organisation.
Les cinq composants ont pour objectif l'amélioration du système du contrôle interne de l'organisation et ils sont interconnectés. Il s'agit de : (l'environnement de contrôle, l'évaluation des risques, les activités de contrôle, l'information et la communication, la surveillance)

1.1.L'environnement de contrôle dans le système d'information (SI)

L'environnement de contrôle englobe l'intégrité et les valeurs éthiques d'une organisation, la philosophie et le style de la direction, la manière dont les compétences et les responsabilités sont attribuées.
Le contrôle interne informatique s'appuie sur l'environnement de contrôle de l'organisation et concerne l'attribution de l'autorité et de la responsabilité des activités. Les solutions de gestion des identités et des accès sont un élément essentiel du dispositif.
Compte tenu des caractéristiques intrinsèques du système d'information, une attention particulière est portée à l'alignement métier du système d'information, aux rôles et responsabilités, aux politiques et procédures et aux compétences techniques. Par exemple, les points de vigilance à adresser sont :

- Le système d'information est souvent considéré comme une organisation séparée des métiers ce qui conduit, à tort, à établir un environnement de contrôle séparé.
- Il est complexe, non seulement en ce qui concerne ses composants techniques, mais aussi en termes d'intégration dans le système de contrôle interne de l'organisation.
- Il peut exposer l'organisation à des risques spécifiques qui exigent des activités de contrôle adéquates pour réduire les risques.
- Il exige des compétences spécialisées qui peuvent être rares.
- Il peut conduire à un niveau de dépendance significatif sur la sous-traitance dans le cas où des processus ou des composants du système d'information seraient externalisés.

1.2.L'Evaluation des risques dans le système d'information :

Dans certains secteurs, l'activité cœur de métier de l'entreprise peut être mise en péril en cas d'arrêt ou de dysfonctionnement de ses systèmes

informatiques, car la dépendance des processus métier envers l'informatique est totale. La gestion des risques informatiques consiste à analyser la connaissance du risque pris par l'entreprise à travers les systèmes informatiques (cartographie du risque informatique), en termes d'impact métier (Legrenzi & Rosé , 2020)
La multiplication des risques lié au contrôle interne est probablement plus importante en ce qui concerne les systèmes d'information que dans d'autres secteurs de l'organisation
L'évaluation des risques intervient :

- Au niveau de l'organisation avec des campagnes d'évaluation des risques des systèmes d'information couvrant le management, la sécurité des données, et le développement.
- Au niveau de chaque activité : l'exploitation des infrastructures, les processus de modification d'une application, …

1.3.L'Activités de contrôle dans le système d'information :

Les activités de contrôle répondent au besoin de politiques, de procédures et d'actions spécifiques pour s'assurer que les objectifs métiers sont atteints. Elles sont mises en œuvre pour traiter les risques. Le COSO imposant la matérialisation factuelle des contrôles.
Il s'agit ici d'activités à tous les niveaux de l'organisation : approbations, compétences, vérifications, réconciliations, évaluations de prestations opérationnelles, surveillance de l'actif et séparation des fonctions.
COBIT identifie deux grands groupes d'activités de contrôle informatique : les contrôles généraux et les contrôles applicatifs.

Les contrôles généraux font référence à ces contrôles pertinents conçus pour s'assurer que l'environnement de contrôle d'une entité est bien géré et appliqué à toutes les tailles de systèmes, sont ceux qui sont intégrés aux processus et aux services informatiques, il concerne par exemple : la gestion des changements, la sécurité et l'exploitation. Alors que les contrôles d'application sont des contrôles automatisés relatifs à des tâches réalisées par le système d'information comprennent le contrôle des entrées, du traitement et des sorties basées sur le flux de traitement des données. En d'autres termes, les contrôles d'application étaient axés sur l'exactitude, l'exhaustivité, la validité et l'autorisation des données saisies, saisies dans le système, traitées, stockées, transmises à d'autres systèmes et déclarées (M.B & P.J, 2009). En outre, les contrôles généraux peuvent être utilisés pour soutenir les contrôles d'application et, par conséquent, permettre au système d'information d'être exploité en amabilité (C & P.C, 2003).

Étant donné que l'information financière dans de nombreuses entités est basée sur des systèmes d'information tels que les systèmes ERP, les contrôles informatiques aident les entités à atteindre l'objectif du contrôle interne. À l'instar de la sécurité de l'information, les contrôles informatiques peuvent également gérer et protéger l'information et les systèmes d'information contre

l'accès, l'utilisation, la divulgation, la perturbation, la modification ou la destruction non autorisés (A & J.H.P, 2007).

1.4.L'Information- communication dans le système d'information :

Ce composant vise à assurer que l'information pertinente est identifiée, recueillie et diffusée dans les délais appropriés afin que l'ensemble du personnel puisse assumer ses responsabilités.

Pour cela, les systèmes d'information doivent garantir que toutes les informations importantes sont collectées de manière fiable et ponctuelle et diffusées convenablement. COBIT prend en compte une très riche segmentation de l'information selon des critères précis (efficacité, efficience, confidentialité, intégrité, disponibilité, conformité et fiabilité) (Carlier, 2019).

1.5.La Surveillance dans le système d'information :

Les systèmes de contrôle interne doivent être supervisés pour évaluer leur qualité et leur performance dans le temps. C'est le « contrôle du contrôle », qui couvre différents types de suivi : le contrôle continu, les évaluations séparées ou une combinaison des deux. Le contrôle continu correspond à la supervision « normale » du management opérationnel. La nécessité de conduire des évaluations séparées (tant en ce qui concerne le contenu que la durée) dépend des résultats de l'analyse de risques et des activités de surveillance continue.

La mesure de la performance répond aux exigences de transparence et de compréhension des coûts, des bénéfices, des stratégies, des politiques et des niveaux de services informatiques offerts conformément aux attentes de la gouvernance des systèmes d'information.

Ces mesures peuvent facilement se traduire par la mise en place d'un BSC (Balance ScoreCard) qui va offrir une vision d'ensemble de la performance.

2- rôle du diapositive du contrôle interne :

La norme IIA 2130 précise les finalités du contrôle interne choisi à faire face aux risques relatifs aux gouvernement d'entreprise, aux opération et système d'information de l'entreprise comme suit (IFACI, 2007):

- La conformité aux lois et règlements ;
- L'atteinte des objectifs stratégiques de l'organisation ;
- La protection des actifs ;
- La fiabilité et l'intégrité des informations financières et opérationnelles

2.1. Conformité aux lois et règlements :

Il s'agit des lois et règlements auxquels la société est soumise. Les lois et les règlements en vigueur fixent des normes de comportement que la société intègre à ses objectifs de conformité.

Compte tenu du grand nombre de domaines existants (droit des sociétés, droit commercial, sécurité, environnement, social, etc.), il est nécessaire que la société dispose d'une organisation lui permettant de :

- Connaître les diverses règles qui lui sont applicables ;
- Être en mesure d'être informée en temps utile des modifications qui leur sont apportées (veille juridique) ;
- Transcrire ces règles dans ses procédures internes ;
- Informer et former des règles qui les concernent.

Le contrôle interne des SI consiste à identifier toutes les lois, réglementations et contrats applicables et le niveau de conformité des SI à cet égard, et optimiser les processus informatiques pour réduire le risque de non-conformité (David & Udays, 2007).

2.2. Application des instructions et des orientations fixées par la Direction Générale ou le Directoire

Les instructions et orientations de la Direction Générale ou du Directoire permettent aux collaborateurs de comprendre ce qui est attendu d'eux et de connaître l'étendue de leur liberté d'action. Ces instructions et orientations doivent être communiquées aux collaborateurs concernés, en fonction des objectifs assignés à chacun d'entre eux, afin de fournir des orientations sur la façon dont les activités devraient être menées. Ces instructions et orientations doivent être établies en fonction des objectifs poursuivis par la société et des risques encourus.

2.3. Bon fonctionnement des processus internes de la société notamment ceux concourant à la sauvegarde des actifs

L'ensemble des processus opérationnels, industriels, commerciaux et financiers sont concernés.

Le bon fonctionnement des processus exige que des normes ou principes de fonctionnement aient été établis et que des indicateurs de performance et de rentabilité aient été mis en place.

Par « actifs », il faut entendre non seulement les « actifs corporels » mais aussi les « actifs incorporels » tels que le savoir-faire, l'image ou la réputation. Ces actifs peuvent disparaître à la suite de vols, fraudes, improductivité, erreurs, ou résulter d'une mauvaise décision de gestion ou d'une faiblesse de contrôle interne. Les processus y afférents devraient faire l'objet d'une attention toute particulière.

Il en va de même des processus qui sont relatifs à l'élaboration et au traitement de l'information comptable et financière. Ces processus comprennent non seulement ceux qui traitent directement de la production des états financiers mais aussi les processus opérationnels qui génèrent des données comptables.

2.4. Fiabilité des informations financières

La fiabilité d'une information financière ne peut s'obtenir que grâce à la mise en place de procédures de contrôle interne susceptibles de saisir fidèlement toutes les opérations que l'organisation réalise.

Le rôle du dispositif de contrôle interne des systèmes d'information lié à cet objectif est décliner comme suit (Farid & Mohamed, 2015):

- Assurer la disponibilité de l'information de façon à ce qu'elle soit accessible en temps voulu et de la manière requise par une personne autorisée.
- Assurer l'intégrité de l'information de manière à ce que celle-ci ne soit pas détruite ou altérée de quelconque façon sans autorisation, et que le support de cette information lui procure la stabilité et la pérennité voulues.
- Limiter la divulgation de l'information aux seules personnes autorisées à en prendre connaissance, assurant ainsi une stricte confidentialité.
- Permettre de confirmer l'identité d'une personne ou l'identification d'un document ou d'un dispositif.
- Se prémunir contre le refus d'une personne de reconnaître sa responsabilité à l'égard d'un document ou d'un autre objet, dont un dispositif d'identification avec lequel elle est en lien.

3- Méthodologie de la recherche :

Dans le but de déterminer le rôle du contrôle interne dans la prévention des risques liées aux systèmes d'information dans les entreprises économiques algériennes nous avons choisi de procéder par une enquête de perception par questionnaire destiné au public concerné, les répondants étaient assurés que les informations fournies resteront strictement anonymes et confidentielles. Comme cela l'étude impliquait des participants humains, une approbation éthique a été obtenue de notre recherche.

Ce questionnaire comporte trois parties, la première concerne les caractéristiques de l'échantillon : Sexe, âge, niveau d'instruction et ancienneté …etc.

La deuxième partie concerne les questions relatives aux rôles du dispositif du contrôle interne dans la prévention des risques liées aux SI au nombre de 23 réparties selon les objectifs du contrôle interne.

Le questionnaire a été élaboré sur la base des objectifs du cadre conceptuel COSO et COBIT. Nous avons suivi les procédures de Dillman (2000) pour concevoir et administrer l'enquête. La plupart des questions étaient sélectionnées et adaptées, si nécessaire, à partir d'instruments existants, à l'aide d'échelles de Likert en cinq modalités de réponses (Pas du tout d'accord, pas d'accord, neutre. D'accord, tout à fait d'accord) que nous sommes analysés par SPSS version 26, l'échelle est présentée comme suit :

Table 1. Échelle de mesure de Likert de cinq modalités

Moyenne pondérée	Niveau
[1.00 - 1.79]	Pas du tout d'accord
[1.80 - 2.59]	Pas d'accord
[2.60 - 3.39]	Neutre
[3.40 - 4.19]	D'accord
[4.25 - 5.00]	Tout à fait d'accord

Source : élaboré par nous-mêmes

SPSS V26 a été utilisé pour évaluer la fiabilité du questionnaire et des sources de données. Le niveau de signification est fixé à 0,05 pour toutes les relations. Afin de vérifier les hypothèses de l'étude, les techniques statistiques suivantes ont été utilisées :

- Statistiques descriptives pour analyser les caractéristiques de l'échantillon ;
- Le coefficient α de Cronbach pour tester la fiabilité des items ;
- Test à un échantillon pour vérifier les hypothèses, dont l'objectif du test T pour l'échantillon unique est de comparer une moyenne observée à une moyenne théorique. Dans le cadre d'une hypothèse univariée, il s'agit, par exemple, de comparer un taux mesuré à une même norme ; pour savoir si la différence est significative (p-value) qui correspond au risque alpha= 5% ; si la valeur absolue de t (|t|) est supérieure à la valeur critique ; alors la différence est significative, dans le cas contraire, elle ne l'est pas.

3.1.Caractéristique de la population ciblée :

La population cible a été sélectionnée à partir de la base de données des grandes entreprises algériennes (DGE) ; les données utilisées dans cette étude ont été recueillies au moyen d'un questionnaire auto-administré entre février 2022 et avril 2022. 50 questionnaires traditionnels et 100 des questionnaires en ligne ont été envoyés à 150 personnes de différentes entreprises. Un total de 56 sur des 150 répondants ont rempli le questionnaire, ce qui représente un taux de réponse de 37,33 %.

Le tableau ci-après résume la répartition de ces répondants selon leurs secteurs d'activités.

Table 2. La répartition des répondants selon leurs secteurs d'activités

Secteurs d'activité	Entreprise	% (n=56)
Service	Groupe GEMA SPA LA FLESH BLEU SPA RAIL LOGISTIQUE SPA AIR ALGERIE SPA TASSILI AIR LINE SPA INFRAFER SPA SNTF SPA EMA	21%
Industrie	Groupe SAIDAL Groupe BIOPHARM Groupe CEVITAL SPA SONACOM	16%
Télécommunication	SPA ALGERIE TELECOM SPA MOBILIS	9%
BTPH	SPA COSIDER Groupe HASNAOUI SPA ENGCB	25%

Energie	SPA ENAGEO SPA ENSP SPA ENAFOR SPA ENTP SPA ENAC SPA SH EXPLO SPA HESP SPA BJSP SPA SARPI SPA ENGTP	29%

Source : résultat de l'analyse par SPSS

En ce qui concerne les emplois occupés par les personnes ciblées, le tableau suivant montre leurs postes dans leurs entreprises.

Table 3. La répartition des répondants en fonction de leur emploi actuel

Poste occupé	% (n=56)
Manager	14%
Responsable de la DSI	5%
DFC	16%
Auditeur des SI	20%
Informaticien	13%
Cadre administratif	23%
Autres	9%

Source : résultat de l'analyse par SPSS

3.2.Validité et fiabilité des échelles de mesure :

3.2.1. Fiabilité des échelles de mesure :

Alpha Cronbach est l'indicateur le plus utilisé pour mesurer la cohérence interne d'un ensemble d'items d'une échelle pour estimer la fiabilité du test statistique et déterminer si elles mesurent bien la même dimension, il ne peut se calculer que sur des données continues, il est compris entre 0 et 1, plus la valeur

d'Alpha de Cronbach approchera de 1, plus la cohérence interne des items est bonne.

Pour tester la validité et la fiabilité des échelles de mesure nous avons calculé le coefficient alpha de Cronbach.

Le coefficient calculé pour les questions est égal à 0,981(98,1%) ce qui nous permet d'affirmer la fiabilité de nos échelles de mesure et ainsi la validité du questionnaire. (Voir Tableau 04 et Tableau 05 ci- dessous)

Table 4. La fiabilité des échelles de mesures du questionnaire

Alpha de Cronbach	Nombre d'éléments
,981	23

Source : résultat de l'analyse par SPSS

Table 5. La fiabilité des échelles de mesures par axes

Axes	Alpha de Cronbach	Nombre d'éléments	Commentaire
Conformité aux lois et règlements	,933	5	Excellent
L'efficacité des opérations	,915	6	Excellent
L'analyse et l'évaluation des risques	,857	4	Bon
La sécurité des actifs et les données	,928	5	Excellent
La qualité de l'information financière	,974	3	Excellent

Source : résultat de l'analyse par SPSS

3.2.2. Validité constructive :

Le coefficient de contingence C de Pearson permet de mesurer la présence ou non d'une relation linéaire entre deux variables quantitatives continues. Par le quel nous volons étudier la corrélation de chaque axe de l'étude avec le degré global du sujet étudié.

Le tableau 06 montre qu'il existe une forte corrélation entre la prévention des risques liées aux systèmes d'information et les différents axes du contrôle interne. Et donc tous les axes du questionnaire sont considérés valides par rapport à leurs objectifs de la présente étude.

Table 6. Facteur de corrélation entre le degré de chacun des axes du questionnaire et le degré global du questionnaire

axes	Sig. (Bilatérale)	Corrélation de Pearson
Conformité aux lois et règlements	,000	,961
L'efficacité des opérations	,000	,967
L'analyse et l'évaluation des risques	,000	,945
La sécurité des actifs et les données	,000	,956
La qualité de l'information financière	,000	,961

Source : résultat de l'analyse par SPSS

3.3.Analyse des résultats et tests d'hypothèses

Nous avons effectué une analyse descriptive des réponses en calculant la moyenne et l'écart-type pour faire sortir les tendances des réponses puis procéder à des tests T de Student afin de vérifier nos hypothèses émises, les résultats par axe du contrôle interne :

3.3.1. Conformité aux lois et règlement :

Afin de vérifier la première hypothèse (H1), un test sur l'échantillon a été réalisé à un niveau alpha de 0,05. Les résultats globaux des mesures sont résumés dans les tableaux suivants.

Table 7. Statistiques sur échantillon uniques

N	Moyenne	Ecart type	Moyenne erreur standard
56	3,8036	1,31922	,17629

Source : résultat de l'analyse par SPSS

Table 8. Résultats des tests T de Student de la conformité aux lois et règlement

T	ddl	Sig. (bilatéral)	Différence moyenne	Intervalle de confiance de la différence à 95 %	
				Inférieur	Supérieur
21,576	55	,000	3,80357	3,4503	4,1569

Source : résultat de l'analyse par SPSS

Ces résultats montrent que la moyenne arithmétique pondérée de la conformité aux lois et règlement est égale à 3.8036 qui correspond au deuxième degré (d'accord) sur échelle de Likert. De plus, les résultats montrent qu'il n'existe pas une différence entre les niveaux d'objectifs liés à conformité aux lois et règlement atteints par les entreprises algériennes étudiées, et les niveaux d'objectifs liés à conformité aux lois et règlement de prévention des risques basée sur le contrôle interne des systèmes d'information ($p < 0,05$). Ce résultat nécessite d'accepter la première hypothèse (H 01) selon laquelle le contrôle interne des systèmes d'information contribue à prévenir les risques des SI à travers la conformité aux instructions de la direction générale, aux lois et règlements ;

3.3.2. L'efficacité des opérations :

Afin de vérifier la deuxième hypothèse (H2), un test sur l'échantillon a été réalisé à un niveau alpha de 0,05. Les résultats globaux des mesures sont résumés dans le tableau suivant.

Table 9. Statistiques sur échantillon uniques

N	Moyenne	Ecart type	Moyenne erreur standard
56	3,5952	1,15420	,15424

Source : résultat de l'analyse par SPSS

Table 10. Résultats des tests T de Student de l'efficacité des opérations

t	ddl	Sig. (bilatéral)	Différence moyenne	Intervalle de confiance de la différence à 95 %	
				Inférieur	Supérieur
23,310	55	,000	3,59524	3,2861	3,9043

Source : résultat de l'analyse par SPSS

Ces résultats montrent que la moyenne arithmétique pondérée du l'alignement stratégique est égale à 3.5952 qui correspond au deuxième degré (d'accord) sur échelle de Likert. De plus, les résultats montrent qu'il n'existe pas une différence significative entre les niveaux d'objectifs liés à l'efficacité des opérations atteints par les entreprises algériennes étudiées, et les niveaux d'objectifs liés à l'efficacité des opérations de prévention des risques basée sur le contrôle interne des systèmes d'information ($p < 0,05$). Ce résultat nécessite d'accepter la deuxième hypothèse (H 02) selon laquelle le contrôle interne des

systèmes d'information contribue à prévenir les risques des SI à travers l'utilisation optimale des ressources affectées et la maîtrise des processus ;

3.3.3. L'analyse et l'évaluation des risques

Afin de vérifier la troisième hypothèse (H3), un test sur l'échantillon a été réalisé à un niveau alpha de 0,05. Les résultats globaux des mesures sont résumés dans le tableau suivant.

Table 11. Statistiques sur échantillon uniques

N	Moyenne	Ecart type	Moyenne erreur standard
56	3,5089	,97813	,13071

Source : résultat de l'analyse par SPSS

Table 12. Résultats des tests T de Student de l'analyse et l'évaluation des risques

t	ddl	Sig. (bilatéral)	Différence moyenne	Intervalle de confiance de la différence à 95 %	
				Inférieur	Supérieur
26,846	55	,000	3,50893	3,2470	3,7709

Source : résultat de l'analyse par SPSS

Ces résultats montrent que la moyenne arithmétique pondérée de l'analyse et l'évaluation des risques est égale à 3.5089 qui correspond au deuxième degré (d'accord) sur échelle de Likert. De plus, les résultats montrent qu'il n'existe pas une différence entre les niveaux d'objectifs liés à l'analyse et l'évaluation des risques atteints par les entreprises algériennes étudiées, et les niveaux d'objectifs liés l'analyse et l'évaluation des risques de prévention des risques basée sur le contrôle interne des systèmes d'information ($p < 0,05$). Ce résultat nécessite d'accepter la troisième hypothèse (H 03) selon laquelle le contrôle interne des systèmes d'information contribue à prévenir les risques des SI à travers l'identification, l'analyse et l'évaluation des risques ;

3.3.4. La sécurité des actifs et les données :

Afin de vérifier la quatrième hypothèse (H4), un test sur l'échantillon a été réalisé à un niveau alpha de 0,05. Les résultats globaux des mesures sont résumés dans le tableau suivant.

Table 13. Statistiques sur échantillon uniques

N	Moyenne	Ecart type	Moyenne erreur standard
56	3,7321	1,05298	,14071

Source : résultat de l'analyse par SPSS

Table 14. Résultats des tests T de Student de la sécurité des actifs et les données

t	ddl	Sig. (bilatéral)	Différence moyenne	Intervalle de confiance de la différence à 95 %	
				Inférieur	Supérieur
26,524	55	,000	3,73214	3,4502	4,0141

Source : résultat de l'analyse par SPSS

Ces résultats montrent que la moyenne arithmétique pondérée de la sécurité des actifs et les données est égale à 3.7321 qui correspond au deuxième degré (d'accord) sur échelle de Likert. De plus, les résultats montrent qu'il n'existe pas une différence entre les niveaux d'objectifs liés à la sécurité des actifs et les données atteintes par les entreprises algériennes étudiées, et les niveaux d'objectifs liés la sécurité des actifs et les données de prévention des risques basée sur le contrôle interne des systèmes d'information ($p < 0,05$). Ce résultat nécessite d'accepter la quatrième hypothèse (H 04) selon laquelle le contrôle interne des systèmes d'information contribue à prévenir les risques des SI à travers la sécurité des actifs et la protection des données ;

3.3.5. La qualité de l'information financière

Afin de vérifier la première sous-hypothèse (H5), un test sur l'échantillon a été réalisé à un niveau alpha de 0,05. Les résultats globaux des mesures sont résumés dans le tableau suivant.

Table 15. Statistiques sur échantillon uniques

N	Moyenne	Ecart type	Moyenne erreur standard
56	3,6667	1,21439	,16228

Source : résultat de l'analyse par SPSS

Table 16. Résultats des tests T de Student de la qualité de l'information financière

t	ddl	Sig. (bilatéral)	Différence moyenne	Intervalle de confiance de la différence à 95 %	
				Inférieur	Supérieur
22,595	55	,000	3,66667	3,3415	3,9919

Source : résultat de l'analyse par SPSS

Ces résultats montrent que la moyenne arithmétique pondérée de la qualité de l'information financière est égale à 3.6667 qui correspond au deuxième degré (d'accord) sur échelle de Likert. De plus, les résultats montrent qu'il n'existe pas une différence entre les niveaux d'objectifs liés à la qualité de l'information financière atteints par les entreprises algériennes étudiées, et les niveaux d'objectifs liés la qualité de l'information financière de prévention des risques basée sur le contrôle interne des systèmes d'information ($p < 0,05$). Ce résultat nécessite d'accepter la cinquième hypothèse (H 05) selon laquelle le contrôle interne des systèmes d'information contribue à prévenir les risques des SI à travers l'amélioration de la qualité de l'information financière, opérationnelle et de gestion.

4-Conclusion:

La mise en place de dispositif de contrôle interne repose en grande partie sur le contrôle de l'informatique. C'est un point de passage obligé. En effet, avec la numérisation des entreprises, la quasi-totalité des procédures repose aujourd'hui sur des traitements informatiques, des serveurs, des bases de données, …. La mise en place de différents dispositifs de contrôle interne efficaces se fait et se fera de plus en plus à l'aide de systèmes d'information conçus à cet effet. Toutes les applications informatiques existantes doivent en tenir compte et le cas échéant doivent être revues pour prendre en compte des règles de contrôle interne et pour, éventuellement, corriger d'éventuelles fragilités des dispositifs de contrôle interne en place.

La loi fait aujourd'hui obligation de mettre en place et de développer des dispositifs de contrôle interne. Ceci exige d'analyser et de perfectionner les principaux processus de l'entreprise et de mettre en place des dispositifs de contrôle interne. C'est le cœur de la démarche. Il est aussi nécessaire de renforcer le contrôle des données car l'expérience montre que c'est un domaine encore fragile qui nécessite des dispositifs de contrôle rigoureux.

Le maintien d'un dispositif de contrôle interne efficace dans le temps ne peut être obtenu que par une bonne gouvernance des systèmes d'information, intégrant la maîtrise des risques et la conformité aux lois et règlements. Le

référentiel CobiT, aujourd'hui apporte aux organisations et à leurs parties prenantes les notions et les outils leur permettant de gouverner efficacement leur système d'information et, de là, de contribuer à l'instauration d'un bon niveau de contrôle interne par l'informatique, en alliant performance et sécurité.
Enfin, l'étude vérifie les hypothèses supposés pour répondre à la problématique de notre sujet. Le tableau 17 résume les résultats obtenus.

Tableau 17 : Les résultats de la vérification des hypothèses

Numéro de la sous-hypothèse	Résultat de la vérification
H01 : Le contrôle interne des systèmes d'information contribue à prévenir les risques des SI à travers la conformité aux instructions de la direction générale, aux lois et règlements ;	**acceptée**
H02 : Le contrôle interne des systèmes d'information contribue à prévenir les risques des SI à travers l'utilisation optimale des ressources affectées et la maîtrise des processus ;	**acceptée**
H03 : Le contrôle interne des systèmes d'information contribue à prévenir les risques des SI à travers l'identification, l'analyse et l'évaluation des risques ;	**acceptée**
H04 : Le contrôle interne des systèmes d'information contribue à prévenir les risques des SI à travers la sécurité des actifs et la protection des données ;	**acceptée**
H05 : Le contrôle interne des systèmes d'information contribue à prévenir les risques des SI à travers l'amélioration de la qualité de l'information financière, opérationnelle et de gestion.	**acceptée**

Source : élaboré par l'étudient

Les résultats obtenues montrent que le contrôle interne à un impact majeur sur la préventions des risques liées aux systèmes d'information, à travers l'élimination de risque d'avoir un manque de fiabilité, de conformité, d'intégrité, de disponibilité et de confidentialité des informations critiques ou sensibles de l'entreprise (données financières, commerciales, personnelles, stratégiques, ou liées au savoir-faire de l'entreprise) et d'avoir à faire face aux

risques numériques sur les applications majeures, les infrastructures clés et les données critiques.

Les entreprises algériennes doivent veiller à :

- S'assurer de la conformité du système d'information mis en place avec les règles et procédures internes fixés par la direction générale ainsi que les lois et règlement fixés par le législateur ;
- Définir les privilèges de manipulation et de consultation sur le SI afin de protéger les données produites par le système d'information et de s'assurer de l'amélioration de la qualité d'information financière et opérationnelle ;
- S'intéresser aux risques informatiques de façon à avoir une bonne connaissance afin de définir l'appétence aux risques informatiques ;
- Définir un plan d'action pour la gestion des risques informatiques ;
- Adopter le référentiel d'audit et de gouvernance des systèmes d'information afin d'assurer une optimisation de l'utilisation du système d'information.

5- Citations:

(ITGI), I. G. (2005). Control objectives,management guidlines,maturity model in Cobit 4.0. Illinois.

A, D., & J.H.P, E. (2007). An information security governance framwork, information systems management. 361-372.

C, F., & P.C, Z. (2003). IT control objectives for Sarbanes-Oxley: the importance of IT in the Designe, implantation and sustainability of internal control over disclosure and financial reporting. IT gouvernance institute.

Carlier, A. (2019). Premiers pas avec le modèle COBIT 5. AFNOR.

David , A., & Valérié, D. (2013). Mesurer la performance du système d'information. EYROLLES.

David, S., & Udays, M. (2007). the importance of the COBIT framework IT process for effective internal control of the reability of financial reporting:an international survy. information systems assurance, 5-7.

Farid, e.-m., & Mohamed, n. (2015). l'audit interne face aux risques de cybersécurité. revue international des auditeurs et controleurs internes, 26-28.

IFACI. (2007). Cadre de référence international des pratioques professionnelles de l'audit interne.

IFACI. (2007). Le dispositif du controle interne: cadre de référence.

J.C, B., & L.E, G. (2002). The effects of decision aid orientation on risk factor identification audit test planning auditing.

Legrenzi, C., & Rosé , P. (2020). Pilotage du SI et de la transformation digitale: les tableaux de bord de la DSI. DUNOD.

M.B, R., & P.J, S. (2009). Accounting information systems. Pearson.