Contribution de l'audit interne dans la gestion des risques liés aux systèmes d'information dans le cadre de la gouvernance des systèmes d'information - Cas Evolutec International – Algérie

مساهمة التدقيق الداخلي في تسيير المخاطر المتعلقة بنظم المعلومات في إطار حوكمة نظم المعلومات – حالة ايفوليتاك انترناسيونال – الجزائر

Abdelouahed Mohamed, Etudiant doctorant en Comptabilité Université Mohamed Khider de Biskra -
Dr Ahmed Gaid Noureddine, Université Mohamed Khider de Biskra

Résumé

De nos jours, les systèmes d'information (SI) dans une entreprise moderne requièrent une importance vitale en ce sens qu'ils conditionnent la réussite, voire même, la pérennité de l'entreprise elle-même. Cependant, assigner des objectifs à atteindre, identifier des besoins, mettre en place une stratégie à long terme serait vain sans une prise en charge adéquate de la gestion des risques SI.

Dans cette optique et, soucieux de mettre en évidence l'importance de la contribution de l'audit interne dans la gestion des risques SI, nous avons procédé à une étude de cas sur terrain au profit d'une entreprise en l'occurrence **Evolutec International, Algérie**. Telle est donc la matrice de réflexion et d'analyse du présent article qui propose une démarche systématique et exhaustive en vue de l'identification et de l'évaluation des risques SI dans le cadre de la gouvernance SI d'une entreprise.

Ce travail de recherche a abouti à des résultats probants et a permis notamment de déceler des défaillances intrinsèques pouvant occasionner une brèche dans l'interface de sécurité des systèmes d'information, particulièrement la confidentialité, et provoquer des dommages conséquents aux actifs de l'entreprise. Notre souci majeur étant de remédier à de pareilles lacunes, nous avons été amenés à faire des recommandations pertinentes en la matière. Il reste à noter que tout au long de ce travail de recherche, nous avons adopté le référentiel spécialisé CObIT (Control Objectives for Information and related

Technology), comme outil de travail technique de base pour l'exécution de l'audit des SI objet de cette étude.
Mots clés: Systèmes d'information, gestion des risques, audit interne, Cobit, gouvernance SI.

ملخص:

في الوقت الحاضر، تعتبر نظم المعلومات ذات أهمية حيوية تحدد نجاح و استمرارية المؤسسة الاقتصادية، إلا انه للتمكن من وضع و تحقيق أهداف ذات أبعاد إستراتيجية لن يكون ذو جدوى دون إدارة و تسيير جيدة لمخاطر نظم المعلومات.

في هذا السياق، نحاول من خلال هذه الورقة البحثية تسليط الضوء على دور و مساهمة التدقيق الداخلي في تسيير المخاطر المتعلقة بنظم المعلومات، و هذا من خلال قيامنا بدراسة ميدانية بمؤسسة Evolutec International بإتباع منهج منظم و متكامل لتحديد و تقييم مخاطر نظم المعلومات في ظل حوكمة هذه الأخيرة.

توصلنا من خلال هذه الورقة البحثية إلى نتائج بالغة الأهمية، من خلال تعريف و تحديد مختلف التهديدات التي يمكن أن تسبب خطرا على نظم المعلومات، وخاصة فيما يتعلق بسريتها و التي يمكن أن تسبب ضررا كبيرا لأصول المؤسسة و بالتالي إستراتيجيتها. إن الهدف من دراستنا هو إبراز مساهمة التدقيق الداخلي في الكشف عن التهديدات و المخاطر المتعلقة بنظم المعلومات، تقييم أثرها و كيفية الحد منها لتحقيق إستراتيجية المؤسسة و هذا من خلال التوصيات المقدمة، مستخدمين مرجعية CobIT (الأهداف الرقابية في المعلومات والتكنولوجيا ذات الصلة) لتنفيذ مهمة التدقيق.
الكلمات المفتاحية: نظم المعلومات، مخاطر نظم المعلومات، تسيير مخاطر نظم المعلومات، التدقيق الداخلي، كوبيت، حوكمة نظم المعلومات.

1. Introduction

La gouvernance des SI consiste de faire correspondre la politique de la gestion du système d'information avec la stratégie globale de l'entreprise[1].Ce système d'information est exposé à des éléments menaçants et soumis à des agressions internes (pannes de matériels, erreurs de manipulations, malveillances internes etc.) et externes (saturation du réseau, action de virus informatiques etc.). De ce fait, la

détermination du niveau de ces risques et leur gestion sont primordiales pour atteindre les objectifs de l'entreprise.

Dans son rôle d'évaluation, d'assurance et de conseil, l'audit interne contribue à la gestion des risques SI afin de donner une assurance sur le niveau de maitrise de ces risques. Ce constat nous amène à poser la question essentielle suivante: Quelle est la contribution de l'audit interne dans la gestion et l'évaluation des risques liés aux SI dans leur gouvernance ?

Les résultats obtenus dans le cadre de ce travail de recherche nous permettent d'ores et déjà d'avoir des réponses qu'on estime pertinentes et très significatives. La démarche que nous avons suivie s'articule autour de trois volets en l'occurrence;

Premier volet: Il définit les objectifs de la gouvernance des SI, la gestion des risques SI et les différents risques liés aux SI.

Second volet: On y aborde la démarche à suivre par l'audit interne dans la gestion et l'évaluation des risques SI.

Troisième volet: Dans lequel il sera procédé à l'audit des risques SI, au sein de l'entreprise Evolutec International, par l'utilisation du référentiel CobiT qui semble le mieux adapté à la résolution de cette problématique et à la présentation des différents résultats et recommandations.

Finalement, il convient de noter que la démarche adoptée quant à l'élaboration d'une base de données fiable et représentative repose sur une approche mixte intégrant judicieusement les aspects qualitatifs et quantitatifs dans le processus de collecte de l'information et impliquant, entre autres, les outils traditionnels tels que les questionnaires et les entretiens avec les responsables SI en plus de nos observations personnelles.

2. Gouvernance SI

La gouvernance des SI est une conséquence du mécanisme de gouvernance d'entreprise[2].Selon CobiT,[3] « La gouvernance des SI relève de la responsabilité des dirigeants et du conseil d'administration. Elle est constituée des structure et processus de commandement et de fonctionnement qui conduisent l'informatique de l'entreprise à soutenir les stratégies et les objectifs de l'entreprise ». Cette vision implique une gestion adaptée des risques et une utilisation adéquate des ressources tout en respectant les intérêts des parties intéressées et le contexte de l'entreprise.

La gouvernance des SI est un outil de maîtrise des risques dont l'objectif est de préserver la valeur acquise par l'entreprise contre tous les écarts pouvant entrainer sa dépréciation ou sa destruction. La gouvernance des SI s'appuie sur cinq[4] piliers dont la gestion des risques SI (fig. 1).

Fig.1 : Les Cinq Piliers de la Gouvernance des Systèmes d'Information

2.1 Gestion des risques liés aux systèmes d'information

Le risque se définit généralement par la possibilité qu'un événement, une action ou une inaction affecte la capacité de l'organisation à atteindre ses objectifs [5]et se mesure en termes de conséquences et de probabilité[6].

La gestion des risques est définie [7] comme étant le processus piloté par le management et qui consiste à appréhender et traiter les risques et opportunités liés aux SI susceptibles d'affecter la capacité de l'entreprise à réaliser ses objectifs.

Dans la mise en place du management global des risques au sein des entreprises, les systèmes d'information acquièrent une importance considérable et sont souvent perçus comme générateurs de risques[8].

Comme exemples illustratifs, citons notamment le cas d'indisponibilité totale ou partielle d'un service censé être fourni par le

système d'information. Manifestement une telle situation représente un risque majeur bien que son origine ne relève pas forcément de la sécurité. Autre exemple, une erreur d'écriture dans une procédure stockée, bien que n'étant pas une attaque à proprement dit mais s'apparente à un risque potentiel qu'il faut prendre très sérieusement en compte.

Dans ce contexte et conformément à la démarche de la gouvernance des systèmes d'information, le management des risques des systèmes d'information est considéré comme un domaine stratégique[9]. Ce statut se justifie principalement par le fait que l'entreprise s'appuie intégralement sur ses ressources informationnelles (systèmes d'information et données) pour atteindre ses objectifs.

Le management des risques spécifiques à l'activité informatique a par conséquent un rôle prépondérant dans le dispositif de protection et de maintien de la capacité opérationnelle de l'entreprise. Pour gérer efficacement les risques inhérents à son système d'information, l'entreprise se doit de respecter les trois règles fondamentales[10] suivantes:

1. Connaître en permanence l'état de ses actifs et des changements associés, des personnels opérationnels (internes et externes), des processus et des contrôles mis en place. Toute cette perception aide les responsables à contrôler efficacement les risques liésaux menaces et aux vulnérabilités.

2. Avoir des dirigeants d'entreprise conscients des menaces inhérentes aux systèmes d'information. Cela implique la gestion des risques au niveau des actifs, des procédures et de la sensibilisation des utilisateurs à la sécurité.

3. Disposer de processus et de structures de gouvernance des risques bien élaborés, impliquant l'entreprise dans sa globalité.

2-2 Risques liés aux systèmes d'information

Le risque du système d'information, comme toute classe de risques a des spécificités propres. Cette notion de risques spécifiques aux systèmes d'information est relativement récente. La plupart des entreprises ont jusqu'à présent appréhendé le risque en déployant une politique basée sur la sécurité face aux menaces directes (virus, intrusion etc.) et sur une assurance contre un certain nombre de risques tels que les catastrophes naturelles, la perte de données, l'arrêt de service et autres.

Pour identifier les risques liés aux systèmes d'information, les auditeurs internes doivent déterminer les sources de risques. Assez souvent, les risques liés aux systèmes d'information se concentrent sur les risques technologiques, bien qu'il en existe d'autres également importants de nature humaine et naturelle.

2.2.1 Les risques technologiques

Le risque technologique [11]se définit comme le dysfonctionnement d'un composant dans une infrastructure IT et pouvant perturber partiellement ou totalement un ou plusieurs services, comme les logiciels malveillants (malware), les virus, les spyware, les spams, les hoax, les sniffers et beaucoup d'autres techniques plus complexes de piratage.

Le risque technologique prend en compte trois paramètres fondamentaux [12]:

a. **La perte d'intégrité :** c'est le résultat d'un changement non autorisé au niveau des données ou de l'infrastructure. Cette perte peut être causée par une action intentionnelle ou accidentelle, telle que la modification d'un programme, le crash d'un support ou un bug. Si la perte d'intégrité n'est pas corrigée, les risques de contamination et de corruption des données augmentent significativement et peuvent induire des prises de décisions erronées au niveau de l'entreprise.

b. **La perte de disponibilité :** c'est la conséquence d'une interruption de service qui affecte directement les utilisateurs et le fonctionnement de l'entreprise. Elle provient d'un dysfonctionnement d'un ou de plusieurs composants de l'infrastructure IT. Les causes les plus fréquentes dans ce cas de figure résultent des erreurs dans la phase d'intégration, du dysfonctionnement des mises à jour ou encore des pannes dans les équipements non sécurisés.

2. **La perte de confidentialité :** elle est provoquée par une vulnérabilité élevée du système d'information et son origine se situe, le plus souvent, au niveau d'une ou de plusieurs défaillances dans le système de protection.

2.2.2 Les risques humains

Le risque humain est de très loin le plus important et le plus dangereux.

La menace humaine sur les infrastructures IT provoque une perte annuelle de plus de 50 milliards de dollars pour les seules entreprises américaines[13]. Il s'agit parfois d'espionnage (vol de fichiers, de données, de code sources et autres), ou de malveillance (employés licenciés ou mécontents pouvant induire une intrusion de virus ou tout simplement la destruction de fichiers), sans oublier les risques de fraude dans les systèmes d'information.

L'erreur humaine représente également une autre source de risque tout aussi importante car ses répercussions peuvent elles aussi affecter le fonctionnement d'un système et donc d'une organisation. Dans ce contexte, quatre types d'erreurs doivent être pris en compte : les erreurs de compréhension, les erreurs d'usage, les erreurs de choix et les erreurs de conception.

2.2.3 Les risques naturels

Les risques climatiques sont les plus importants à considérer dans la catégorie des risques naturels et dont les principaux sont [14]:

- L'inondation : c'est un risque fréquent et potentiellement dévastateur pour les infrastructures IT.
- Le gel : risque qui reste lié à la rupture des systèmes de chauffage.
- La canicule : risque lié à la rupture des systèmes de refroidissement.

3. Audit interne dans la gestion des risques SI

L'Audit Interne est défini [15] comme une **activité indépendante et objective** qui donne à l'entreprise une assurance sur le degré de maîtrise de ses opérations, lui apporte des conseils pour les améliorer et contribue à créer de la valeur ajoutée.

Il aide l'entreprise à atteindre ses objectifs en évaluant, par une **approche systématique et méthodique,** ses processus de management des risques, de contrôle et de gouvernement d'entreprise à travers des propositions pour renforcer leur efficacité.

Selon la norme 2120.A1 [16] « L'audit interne doit évaluer les risques afférents au gouvernement d'entreprise, aux opérations et aux systèmes d'information de l'entreprise ». De ce fait, et relativement aux

risques SI, le rôle principal de l'audit interne consiste à évaluer les risques SI pour donner à l'entreprise une assurance objective que sa gestion est efficace,

Dans le cadre de la gouvernance des SI, CobiT est un référentiel spécialisé pour auditer l'activité du SI[17].Il permet aux entreprises d'exploiter au mieux les systèmes d'information tout en maintenant l'équilibre entre la réalisation de bénéfices, l'optimisation des niveaux de risque et l'utilisation des ressources.

CobiT est composé de 37 processus liés aux SI[18], incluant le processus de planification et d'organisation PO.12 relatif à l'évaluation et la gestion des risques SI, que l'auditeur interne doit suivre selon les étapes ci-dessous énumérées [19] :

Référentiel de gestion des risques informatiques: Cela consiste à mettre en place un référentiel de gestion des risques informatiques aligné sur le référentiel de gestion des risques de l'entreprise.

Etablissement du contexte du risque: Cette étape consiste à établir le contexte dans lequel s'applique le cadre d'évaluation du risque afin d'obtenir les résultats appropriés. Cette démarche implique la détermination des contextes interne et externe de chaque évaluation du risque, le but ainsi que les critères de cette évaluation.

3.1 Identification des événements

Ce protocole opérationnel consiste à identifier les événements (menaces importantes et réalistes découlant d'une ou plusieurs vulnérabilités applicables significatives) qui peuvent avoir un impact négatif sur les objectifs ou les opérations de l'entreprise, y compris l'activité, les aspects réglementaires et légaux, la technologie, les partenaires commerciaux, les ressources humaines et le secteur opérationnel. Il s'agit alors de déterminer la nature des conséquences, d'actualiser cette information d'enregistrer et détenir à jour les données sur les risques significatifs dans un registre des risques.

3.2 Évaluation du risque

L'évaluation d'un risque est un point capital dans la gestion des risques des systèmes d'information car elle permet de définir les actions prioritaires. Cette évaluation ne peut être objective sans un diagnostic exact des risques et c'est dans ce cadre que se définit le processus de l'évaluation des risques.

Ce processus consiste à définir [20] l'ordre de priorité des risques en vue d'actions ultérieures, par évaluation et combinaison de leur probabilité d'occurrence et de leur impact sur le système d'information et sur les objectifs SI. Selon la taille de l'entreprise et l'étendue de son activité, on distingue, selon le cas, trois ou cinq niveaux de risque catégorisés comme suit:

- Echelle à trois niveaux[21] : faible, moyen et élevé.
- Echelle à cinq niveaux: minimum, faible, acceptable, élevé, intolérable.

La classification du risque se fait sur une échelle de 1 à 100 et se calcule à partir d'une matrice 3x3 ou 5x5 selon le cas. Pour les échelles à 3 niveaux, la classification s'effectue de la manière suivante :

- Faible : de 0 à 10
- Moyen : de 11 à 50
- Elevé : de 51 à 100

L'évaluation se fait par le calcul de la probabilité et les conséquences de tous les risques identifiés en utilisant des méthodes qualitatives et quantitatives à travers une matrice de risques et un tableau de classification.

Risque = Probabilité x Impact			
Probabilité	Impact		
	Risque faible (10)	Risque moyen (50)	Risque élevé (100)
Faible (0.1)	1	5	10
Moyenne(0.5)	5	25	50
Elevée (1)	10	50	100

Tableau 1: Matrice de calcul 3x3 pour la classification du risque [22]

3.3 Réponse au risque

Pour répondre efficacement à un risque, il faut développer et tenir à jour un processus qui puisse assurer que des contrôles réduisent en permanence l'exposition aux risques. Ce processus doit proposer des stratégies comme l'évitement, la réduction, le partage, l'acceptation, ainsi que la détermination des responsabilités connexes et tenir compte des niveaux de tolérance au risque.

3.6 Maintenance et surveillance d'un plan d'action contre les risques

Un tel plan s'articule autour des axes suivants :

- Établir les priorités et planifier les activités de contrôle à tous les niveaux pour mettre en place les réponses adéquates aux risques inévitables.

- Obtenir l'approbation pour les actions recommandées et l'acceptation de tous les risques résiduels,

- S'assurer que les propriétaires des processus affectés par le risque assument aussi la propriété des actions entreprises.

- Surveiller l'exécution des plans et signaler tout écart au management.

4. Analyses et résultats de l'audit interne des risques SI dans l'entreprise Evolutec International

Avant d'examiner les résultats de cette étude, il faut bien mettre l'accent sur les points suivants [23]:

- L'audit interne ne doit en aucun cas gérer un quelconque risque au nom de la direction.

- L'audit interne doit formuler des conseils, contester ou au contraire appuyer les décisions de la direction, mais en aucun cas prendre des décisions concernant la gestion des risques.

- L'audit interne ne peut pas donner d'assurance objective pour tous les volets du cadre de gestion des risques dont il est responsable. Une telle assurance reste de la responsabilité d'autres parties ou partenaires.

- Toute tâche sortant du cadre des activités d'assurance doit être considérée comme une mission de conseil et doit respecter les normes régissant ce type de mission.

Suivant le processus de la gestion et d'évaluation des risques SI du référentiel CobiT, une mission d'audit a été conduite. Les résultats relevés pour chaque volet du processus audité sont présentés ci-dessous.

4-1 Référentiel de gestion des risques informatiques

La direction générale et le service informatique et télécommunication (IT) de l'entreprise ont mis une politique concernant les règles d'utilisation des ressources informatiques, pour limiter les risques inhérents aux SI et s'aligner sur la politique globale de l'entreprise afin qu'elle puisse atteindre ses objectifs stratégiques.

Cependant cette politique est essentiellement axée sur les risques technologiques et humains en omettant les aléas et risques naturels.

4.2 Établissement du contexte du risque

Dans le contexte de la gouvernance des SI dans l'entreprise, l'objectif est d'auditer la gestion de ses risques SI afin de réaliser les objectifs de l'entreprise. Chaque risque est évalué selon la catégorie à laquelle il appartient (risques technologiques, humains ou naturels).Les critères d'évaluation sont la probabilité, l'impact potentiel et les types de pertes possibles (disponibilité, confidentialité et intégrité).

4. 3 Identification des événements

Dans le contexte de la politique de l'entreprise vis-à-vis des règles d'utilisation des ressources informatiques, chaque risque lié au SI remarqué et observé par les employés doit être signalé dans une fiche de demande d'intervention qui sera adressée au service IT. Ce dernier enregistre le risque signalé dans le registre de risques, sa nature et les moyens utilisés pour le neutraliser.

Sur la base des chiffres recueillis sur le registre des risques durant deux années consécutives (2014-2015) et selon le nombre d'interventions sur l'actif SI de l'entreprise, les risques peuvent être classés comme suit :

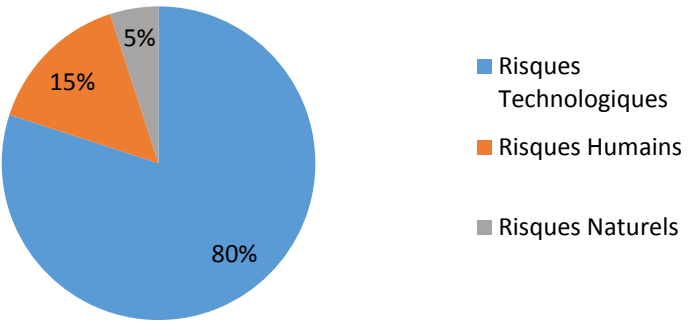

Fig. 2 : Identification des risques SI – Evolutec International

4.4 Évaluation des risques SI

L'entreprise n'effectue pas d'évaluations quantitatives des risques, bien que cette action soit primordiale pour quantifier la probabilité et l'impact des risques constatés, mieux les comprendre et prendre des mesures de protection.

Evolutec International étant une entreprise de taille moyenne (140 employés), le choix d'une matrice d'évaluation d'échelle 3x3 paraît convenable. La classification retenue est présentée dans le tableau suivant:

Catégories	Nature	Enoncé du risque	Type de perte	Quantification de l'impact	Probabilité	Niveau de risque
Risques technologiques	Software	Absence d'antivirus	Perte de confidentialité	95	0.9	85.5 Elevé
	Software	Logiciels piratés	Perte de Disponibilité	50	0.5	25 Moyen
	Hardware	Matériels technologiquement dépassés	Perte de disponibilité	50	0.5	25 Moyen
	Hardware	Coupure d'électricité	Perte de disponibilité	50	0.5	25 Moyen
Risques humains	Données	Fautes de frappe	Perte d'intégrité	50	0.5	25 Moyen
	Données	Téléchargements Hors travail	Perte de confidentialité	90	0.9	81 Elevé
	Manipulation	Introduction de virus via USB	Perte de confidentialité	90	0.9	81 Elevé
	Organisation	Absence du personnel	Perte de disponibilité	100	0.9	90 Elevé
Risques naturels	Poussière	Pertes d'actifs	Perte de disponibilité	10	0.5	2 Faible

Tableau 2 : Classification et évaluation des risques SI – Evolutec International
Source : Construction personnelle

Les constats relevés selon la catégorie du risque se présentent comme suit :

Risques technologiques : L'absence d'antivirus adéquats dans 95% des postes opérationnels fragilise l'ensemble des processus à caractère logiciel et/ou matériel et expose l'entreprise à des risques élevés à l'égard de son actif SI. Cette faille rend possible l'intrusion de virus pouvant causer des pertes de disponibilité.

D'autre part, l'entreprise s'expose à des risques de moyen impact, comme les coupures et l'instabilité de l'alimentation électrique. Ce risque peut causer des pertes importantes notamment au niveau des onduleurs. En outre, la vétusté des actifs représente un facteur de ralentissement des ordinateurs et occasionne des pertes de disponibilité.

Risques humains : Dans cette catégorie de risques, l'intrusion de virus de manière accidentelle ou malveillante par des opérateurs humains via des clés USB ajouté aux téléchargements fréquents et non sécurisés depuis des sites non fiables représente un risque majeur et expose les données de l'entreprise à des pertes de confidentialité.

Notons pour finir que l'absence de personnel SI qualifié représente un risque de grande probabilité et d'impact élevé et qui peut, à tout moment, occasionner d'importantes pertes de disponibilité.

Risques Naturels : De manière générale, l'environnement dans lequel opèrent les actifs informatiques jouent un rôle prépondérant dans le maintien des machines en bon état de fonctionnement. Manifestement, il représente un facteur défavorable pour l'entreprise auditée car elle se trouve dans une zone industrielle et donc exposée à divers agents corrosifs tels que la poussière, le bruit et autres facteurs externes. Cependant le risque de perte de disponibilité demeure faible mais nécessite néanmoins beaucoup d'attention.

4.5 Réponse au risque

L'entreprise tente d'utiliser des stratégies d'évitement pour parer à certains risques par le renouvèlement des équipements matériels et la mise à jour des logiciels spécialisés et ce, afin d'éviter les risques d'obsolescence technologique. Cependant, elle réagit mal ou pas du tout face à d'autres risques jugés élevés tels que l'absence d'antivirus avec licence ou les téléchargements intempestifs opérés par ses employés.

4.6 Maintenance et surveillance d'un plan d'action vis-à-vis des risques

Le service IT exécute des actions planifiées de vérification et de maintenance sur tout l'actif SI régulièrement pendant chaque mois sur l'ensemble de l'actif SI.

Nous avons constaté que les agents du service IT assument la responsabilité de maintenance des actifs SI partiellement ou complètement dégradés suite à des actions inappropriées émanant d'autres employés.

Conclusion

La mise en œuvre de cette méthodologie de l'audit interne dans la gestion des risques SI devrait non seulement améliorer l'efficience et l'efficacité de la gestion des risques SI, mais mettre en exergue également l'apport et le rôle unique que l'audit interne dans le processus d'identification des événements ou des incidents pouvant affecter la capacité de l'entreprise à atteindre ses objectifs.

L'utilisation du référentiel CobiT nous a permis non seulement de bien identifier les différents risques SI mais elle nous a aussi grandement aidés à évaluer les niveaux de risques afin de pouvoir mieux les éviter. Ce référentiel aide les auditeurs internes à appréhender de manière claire et significative les risques encourus quant à l'intégrité et la sécurité des dispositifs et systèmes mis en place en vue de l'exécution de la stratégie, donc assurer la bonne gouvernance des SI de l'entreprise.

En termes de recommandations et dans le but de pallier aux différentes failles et défaillances recensées dans le cadre de cette étude, nous mettons en avant principalement ce qui suit :

- Assurer et de manière continue au personnel concerné des formations spécialisées sur l'audit des systèmes d'information et la gestion des risques de sorte à élever leur niveau de maitrise des protocoles à suivre en vue de renforcer la sécurité de leurs systèmes.

- Evaluer de façon continue les risques des systèmes d'information en utilisant les processus de CobiT.

- Sensibiliser les employés à la valeur des actifs informatiques et prendre des mesures coercitives à l'encontre de ceux qui se rendent responsables des pertes pour l'entreprise.

- Acquérir des licences de protection (antivirus, etc.) pour protéger la confidentialité et limiter les pertes de disponibilité.

- Mettre en place la gouvernance des SI qui repose sur la mise en œuvre des bonnes pratiques dont le référentiel CobiT qui permet à l'entreprise de s'assurer que les risques liés au système d'information sont sous contrôle.

- Dresser un plan d'action contre les risques SI et s'assurer de sa mise à jour régulière en procédant systématiquement à des réajustements appropriés.

- Mettre en place un référentiel de gestion des risques SI.

- Prendre des mesures immédiates adéquates afin de pallier aux risques jugés particulièrement élevés.

Bibliographie

[1]Carpentier, J-F., La gouvernance du système d'information dans les PME, Editions ENI, France, 2010, p.12

[2]Georgel, F., IT Gouvernance, Dunod, Paris, France, 2006, 2ème edition, p.24

[3]Moisand, D. et col, CobiT: Pour une meilleure gouvernance des systèmes d'information, Eyrolles, Paris, France, 2010, 2ème édition, p.05.

[4]Ibid, p.07.

[5]Association pour le Management des Risques et des Assurances en Entreprises(AMRAE), Club de la Sécurité d'Information Français (CLUSIF), Risk Manager et Responsable Sécurité du Système d'Information : Deux métiers s'unissent pour la gestion des risques liés au système d'information, Paris, 2006, p.18

[6]IIA, Le rôle de l'audit interne dans le management des risques de l'entreprise, https://na.theiia.org, 25/09/2015

[7]Kurt F. Reding et col, « Les risques et les contrôles des systèmes d'information » in Manuel d'audit interne, Eyrolles, Paris, France, 2015, 3ème édition, p.15

[8]Zaghloul, A., Information et gestion des risques, Mémoire Master : Sécurité et Gestion des Risques, p.26, Université Hassan 1er de Settat, Maroc, 2010.

[9]Georgel, F., Op. cit, p.85

[10]Carpentier, J-F., Op.cit, p.24

[11]Georgel, F., Op. cit, p.94

[12]Ibid, p.95

[13]Ibid, p.93

[14]Ibid, p.96

[15]Définitions de l'audit et du contrôle internes,http://www.ifaci.com/ifaci/connaitre-l-audit-et-le-controle-interne/definitions-de-l-audit-et-du-controle-internes-78.html 22/09/2015

[16] IIA, Normes pour la pratique professionnelle de l'audit interne, www.theiia.org/chapters/pubdocs/278/normes.pdf15/09/2015
[17]Carpentier, J-F., Op. cit, p.47
[18]ISACA, CobiT 5, http://www.isaca.org/cobit/pages/cobit-5-french.aspx, 22/09/2015
[19]AFAI, Guide d'audit des systèmes d'information, p.99, 2008.
[20]El Oumri, H., Mise en place d'une démarche personnalisée de gestion des risques IT pour DELOITTE, Maroc
[21]Gerogel, F., Op. cit, p.97
[22]Ibid, p.97
[23]IIA, Le rôle de l'audit interne dans le management des risques de l'entrepriseshttps://na.theiia.org, 25/09/2015