Revue du Contrôle de la Comptabilité et de l'Audit
ISSN: 2550-469X
Volume 4 : numéro 2

Une vue d'ensemble sur l'évaluation des risques et analyse de la relation entre l'environnement de contrôle, le potentiel de fraude et les objectifs de contrôle interne

An overview on risk assessment and analysis of the relationship between control environment, fraud potential and internal control objectives.

ERREIMI Meryem
Doctorante
Ecole Nationale de Commerce et de Gestion, Kénitra
Université Ibn Tofail
Laboratoire de recherche en sciences de gestion des organisations
Maroc
meryem.erreimi@uit.ac.ma

KADOURI Abdillah
Enseignant chercheur
Ecole Nationale de Commerce et de Gestion, Kénitra
Université Ibn Tofail
Laboratoire de recherche en sciences de gestion des organisations
Maroc
kadouriabdillah@yahoo.fr

Date de soumission : 14/02/2020

Date d'acceptation : 25/03/2020

Pour citer cet article :

ERREIMI. M & KADOURI. A (2020) «Une vue d'ensemble sur l'évaluation des risques et analyse de la relation entre l'environnement de contrôle, le potentiel de fraude et les objectifs de contrôle interne», Revue du contrôle, de la comptabilité et de l'audit « Volume 4 : numéro 2 » pp : 196 - 218

Digital Object Identifier : https://doi.org/10.5281/zenodo.3732193

Résumé

Depuis le siècle dernier, les organisations publiques et privées s'intéressent de plus en plus au contrôle interne car il s'avère une pratique managériale incontournable pour atteindre les objectifs des organisations, notamment à travers la sauvegarde du patrimoine, la réalisation des opérations avec efficacité et efficience, le maintien du respect des lois et des règlements et la conservation de la fiabilité des rapports financiers ou non financiers. Toutefois, un système de contrôle interne efficace est aussi celui qui permet aux organisations de contrecarrer les risques, d'éviter les fraudes et d'accompagner les changements grâce à un processus d'identification et d'analyse des risques.

À cet effet, toutes les organisations, surtout celles relevant du secteur public, sont mises au défi de renouveler leurs pratiques de management, et de s'orienter vers une démarche de maîtrise des risques à travers l'implémentation d'un système de contrôle interne efficace, dans le but de faire preuve d'une bonne gestion des ressources, d'une plus grande transparence et d'une meilleure qualité des services.

Mots clés : contrôle interne; risque ; évaluation des risques ; fraude ; changement.

Abstract

Since the last century, public and private organizations have become increasingly interested in internal control. This managerial practice has proven to be essential to achieve the organization's objectives, in particular through the safeguarding of assets, carrying out of operations effectively and efficiently, maintaining compliance with laws and regulations and conserving the reliability of financial and non-financial reports. However, an effective internal control system is also one that allows organizations to counter risks, prevent fraud and support change through a risk identification and analysis process.

To this end, all organizations, especially those in the public sector, are challenged to renew their management practices, and to move towards a risk management approach through the implementation of an efficient internal control system in order to demonstrate good management of resources, greater transparency and better quality of services.

Keywords : internal control; risk; risk assessment; fraud; change.

Introduction

L'activité économique de toute organisation est porteuse de risques qui peuvent mettre en péril sa pérennité et son existence, et entraver la réalisation de ses objectifs si elle n'agit pas au moment opportun.

Devant cette présence constante de risques, l'organisation doit chercher à mettre en œuvre des actions visant à les maîtriser le mieux possible. Le système de contrôle interne est alors l'ensemble de dispositifs ayant pour but d'assurer la maîtrise des activités et le respect des règles à tous les niveaux.

Le contrôle interne est une notion qui suscite l'intérêt des chercheurs et des praticiens depuis le début du siècle dernier et qui connait un essor considérable au niveau des pratiques managériales récentes. En effet, un système de contrôle interne englobe les mesures, les outils, et les procédés mis en place par la direction de l'organisation, qui, adoptées par l'ensemble du personnel et intégrées au processus de travail, aident à gérer les risques et garantir le déroulement correct des activités.

Un contrôle interne efficace fait partie intégrante du processus de gestion. En effet, le contrôle interne favorise l'efficacité et l'efficience des opérations, réduit le risque de perte d'actifs, contribue à garantir le respect des lois et des réglementations, mais également il assure la fiabilité des informations financières.

Les chercheurs et les praticiens s'accordent sur l'existence de cinq composantes auxquelles il convient de s'intéresser quand on envisage la mise en place d'un système de contrôle interne au sein d'une organisation. Ces composantes ont été définies et décrites pour la première fois en 1992, par le référentiel de contrôle interne COSO[1].

Les cinq composantes fondamentales du contrôle interne sont respectivement:

- L'environnement de contrôle
- L'évaluation des risques
- Les activités de contrôle
- L'information et communication
- Le pilotage

[1] Le COSO est un référentiel de contrôle interne défini par le Committee Of Sponsoring Organizations of the Treadway Commission.

Ces composantes ont été symboliquement représentées sous la forme d'un cube, communément connu sous le nom de « Cube de COSO » (voir figure n°1), et sont inter-reliées entre elles.

Figure N°1 : le cube de COSO

Source : www.coso.org

À travers le présent article, nous tenons à répondre aux questions suivantes : Comment le contrôle interne permet-il aux organisations d'éviter les différents types de risques auxquelles elles sont exposées, notamment ceux relatifs à la fraude et au changement ? Et quelle est la relation entre l'environnement de contrôle d'une organisation, le potentiel de réalisation d'actes frauduleux et la réalisation des objectifs du contrôle interne ?

En réponse à ces questions, nous essayerons de définir dans un premier temps, la notion de risque tant qu'au niveau étymologique que sur le plan organisationnel, ensuite, nous nous intéresserons aux différentes étapes qui composent le processus d'évaluation des risques, tel qu'il était présenté par le référentiel COSO de contrôle interne. Par la suite, nous nous pencherons vers la question de la fraude comme étant un des risques majeurs que confrontent les organisations publiques et privées au quotidien, en exposant les causes des actes frauduleux et en proposant un modèle qui démontre la relation causale entre un environnement de contrôle défavorable, l'apparition de la fraude et l'atteinte à la réalisation des objectifs de contrôle interne. Finalement, nous évoquerons le changement en tant que facteur non négligeable dans le processus d'évaluation des risques.

1. La notion du risque :

Chaque organisation, qu'elle soit privée ou publique, grande ou petite, fait face à des risques de sources externes et internes qui doivent être évalués (COSO, 1992).

Ainsi, pour mettre en place un système de contrôle interne efficace, il faut connaître les risques susceptibles de faire obstacle à l'organisation. Les responsables doivent donc être en veille constante par rapport aux risques auxquels leur organisation fait face.

Mais avant d'évoquer la deuxième composante du contrôle interne, qui est l'évaluation des risques, nous jugeons nécessaire de nous arrêter sur la notion de « risque ».

Le risque est un concept dont l'ambiguïté intrinsèque rend difficile à cerner, à la fois sur le plan ontologique et épistémologique (Kermisch, 2012). De ce fait, il n'existe pas un consensus sur la façon dont le concept de risque doit être défini et interprété (Aven, 2011).

LeRay (2012) énonce que le risque survient lors de la présence simultanée et non prévue d'un aléa et d'une cible, créant ainsi une zone à risque(s). Hadji Rezai (2017) rejoint la même approche, en affirmant que le risque survient lors de la présence simultanée, non prévue et incertaine d'un aléa et d'une cible, ayant pour effet, un écart positif et/ou négatif par rapport à l'atteinte des objectifs de la cible.

Pour Rosa (1998), le risque représente « *une situation ou un événement où quelque chose qui présente de la valeur pour les hommes (y compris les hommes eux-mêmes) est mis en jeu et dont le résultat est incertain.* », dans la même optique, Aven et Renn (2009) définissent le risque comme suit : « *Le risque fait référence à l'incertitude, et à la gravité des événements et des conséquences (ou résultats) d'une activité par rapport à quelque chose que les humains apprécient* ».

Nous remarquons alors dans un premier temps que le terme « risque » est fortement associé à la présence d'incertitude (Smit, 2012). Le risque est un évènement qui peut, ou ne peut pas se produire. Il revêt un caractère inattendu, fortuit ou périlleux (Hightower, 2009), car lorsqu'un risque se réalise, il ne s'agit plus d'un risque, mais d'un sinistre (Caeymaex, 2007) lorsqu'il cause un préjudice ou une perte. Cependant, le risque peut potentiellement parfois causer un gain ou un profit (Novembre et Leanza, 2015).

Le risque est également un évènement inévitable (Sanne, 2008), et se caractérise par un ensemble d'éléments qui composent celui-ci. Pour Kumamoto et Henley (1996), le risque est une combinaison de cinq éléments : la conséquence, la probabilité, l'importance, le scénario causal et la population affectée. Pour sa part, l'ISO (2002) a décrit le risque comme étant la combinaison de probabilité d'évènement et de sa conséquence. Cette vision est partagée par

Nissanke et Dammag (2002), qui stipulent que les risques se caractérisent par leur probabilité de réalisation et leur impact probable une fois qu'ils se réalisent.

Compte tenu de ce qui précède, nous pouvons constater que le terme «risque organisationnel» peut être pareillement associé à la présence d'incertitude. Ceci dit, le risque organisationnel peut être considéré comme un ensemble d'événements incertains qui risquent potentiellement de se produire dans une organisation (Wood, 1964 ; Remenyi et Heafield, 1996), et qui auront un impact sur la réalisation des objectifs de l'organisation une fois qu'ils se produisent, qu'ils soient positifs ou négatifs (IIA, 2003 ; Smit, 2012).

En outre, le risque organisationnel est de nature subjective (Hillson, 2002 ; Vatsa, 2004), ce qui signifie qu'un risque organisationnel jugé certain dans une organisation ne sera pas nécessairement le même que celui d'une autre organisation (Spekmanet Davis, 2004). Par conséquent, l'impact potentiel du risque organisationnel sur la réalisation des objectifs d'une organisation sera unique (Archbold, 2005; Weber et al. 2010).

Bien que les risques organisationnels soient inévitables et de nature assez large (Ritchie et Brindley, 2007), les chercheurs démontrent que les risques organisationnels peuvent être divisés en quatre catégories, à savoir: 1) les risques stratégiques, 2) les risques opérationnels, 3) les risques liés au reporting et 4) les risques de conformité (Remenyi et Heafield, 1996 ; Tchankova, 2002; Smit, 2012; Bruwer et al., 2013; Sin et Ng, 2013) :

1) **Les risques stratégiques** : Ces risques ont un impact direct sur la réalisation de la mission et de la vision de l'organisation. Les objectifs stratégiques qui découlent de la mission et de la vision de l'organisation, fixent les bases des objectifs opérationnels, de reporting et de conformité que l'organisation doit atteindre.
2) **Les risques opérationnels** : Ces risques ont une influence directe sur l'efficacité et l'efficience des opérations par rapport à la manière dont les ressources de l'organisation sont utilisées pour atteindre les objectifs organisationnels.
3) **Les risques liés au reporting** : Ces risques ont une influence directe sur la fiabilité des informations financières ou non financières, qui sont communiqués aux parties prenantes concernées.
4) **Les risques de conformité** : Ces risques ont un impact direct sur la conformité de l'organisation avec la législation en vigueur, les règles, les politiques et les procédures.

En raison de la nature expansive des risques organisationnels, nous pouvons soutenir qu'ils auront une influence imminente sur la réalisation globale des objectifs organisationnels, affectant directement entre autres, la rentabilité, la solvabilité, la liquidité et l'efficacité d'une organisation et de toute évidence l'existence d'une organisation (Luís et al., 2015;Prinsloo et al., 2015).

Cela n'est pas surprenant, car des études antérieures (Bhimani, 2009 ; Buys, 2012) révèlent que l'atténuation inefficace des risques indique souvent une faiblesse au niveau de la gouvernance d'entreprise et un ton inapproprié donné par la direction, servant de preuve de défaillance de l'environnement de contrôle de l'organisation (Schwartz et al., 2005; Grebe, 2014; Kommunuri et al., 2014).

De ce fait, chaque organisation doit chercher à comprendre la nature des risques auxquels elle fait face et à adopter une approche vigilante vis-à-vis de celui-ci (Hightower, 2009).

2. Le processus d'évaluation des risques

La raison d'être du contrôle interne est de permettre à chaque organisation d'atteindre ses objectifs. Or, les risques constituent l'effet de l'incertitude sur l'atteinte des objectifs (ISO, 2009). L'évaluation des risques en tant que composante de contrôle interne permet d'anticiper l'imprévu (Hightower, 2009), et consiste à l'identifier et analyser les risques pertinents associés à la réalisation des objectifs de gestion (Theofanis, et al 2011).

Une approche similaire considère l'évaluation des risques comme le processus d'identification et d'analyse des risques de gestion pertinents, pour atteindre les objectifs de l'organisation (Hightower, 2009), et qui a pour but de produire des états financiers fidèles conformément aux principes comptables (Sudsomboon et Ussahawanitchakit, 2009).

Selon Oseifuah et Gyekye (2013), l'évaluation des risques est l'identification des facteurs qui menacent la réalisation des objectifs d'une organisation. Elle implique l'identification des risques liés à l'efficacité et l'efficience des opérations, à la fiabilité des rapports financiers et au respect des lois et règlements.

Une condition préalable à l'évaluation des risques est l'établissement d'objectifs liés à différents niveaux et cohérents en interne (COSO, 1992). Le processus d'évaluation des risques implique les éléments suivants :

2.1. L'identification des risques

Il s'agit de recenser les différents risques susceptibles d'entraver la réalisation des objectifs de l'organisation. Cette phase consiste à identifier les risques liés aux objectifs clés de l'organisation, et ceux associés aux objectifs de contrôle (DiNapoli, 2007). Ce qui permet à l'organisation de déterminer les événements qui menaceraient la réalisation de chacun de ces objectifs respectifs.

L'identification des risques doit prendre en compte les risques dus à des facteurs internes et externes, à la fois au niveau de l'organisation et à celui des activités (INTOSAI, 2004).

Une fois les risques identifiés, la direction doit les analyser en tenant compte de leur impact (ou leur importance), la probabilité de leur survenance et de déterminer la façon de les gérer.

2.2. L'analyse des risques

Pour déterminer la façon avec laquelle les risques doivent être gérés, il ne suffit pas seulement d'identifier et lister ces risques, mais il faut procéder à leur analyse.

Ainsi, Kaplan et Garrick (1981) déterminent le risque comme un ensemble de scénarii pour chacun desquels sont associées une probabilité (vraisemblance) et une conséquence (impact).Les risques sont alors analysés, tant en fonction de leur probabilité de survenance que de leur impact (DiNapoli, 2007) :

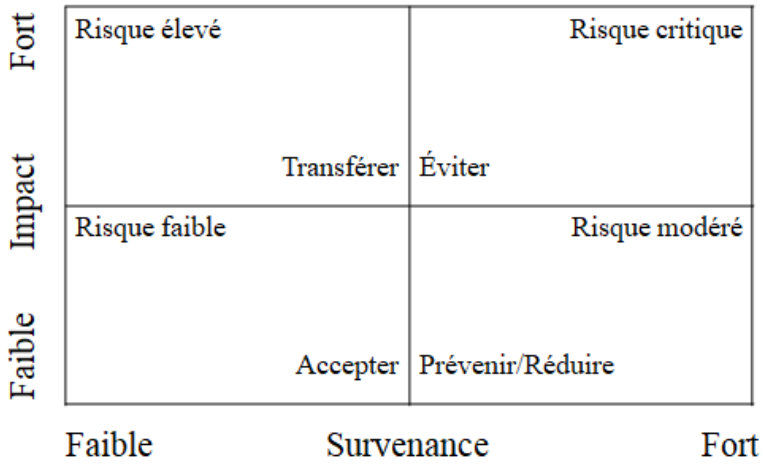
- La probabilité de survenance : elle désigne la possibilité que quelque chose se produise (AFNOR, 2010). Il s'agit de la probabilité qu'un événement défavorable se produise s'il n'y avait pas d'activités de contrôle pour prévenir ou réduire le risque (DiNapoli, 2007). Une probabilité de survenance doit être estimée pour chaque risque identifié.

- L'impact : constitue l'effet qu'un événement aurait sur l'organisation (DiNapoli, 2007). Il s'agit de l'impact des conséquences de l'aléa redouté sur les objectifs de la cible si le risque survient (Le Ray, 2012). L'impact doit être quantifié au mesure du possible et décrit en termes suffisamment précis pour indiquer l'importance du risque (DiNapoli, 2007).

Le niveau du risque ou « l'importance du risque » est estimé alors en multipliant l'impact par la probabilité de survenance. C'est ce qu'on appelle la criticité du risque (AFNOR, 2010).

À travers cette analyse, l'organisation peut classer les risques selon leur degré d'impact et de survenance, de manière à présenter à la direction des informations utiles à la prise de décision quant aux risques qui doivent être gérés de façon prioritaire. Le but majeur de l'analyse des risques réside alors, dans l'identification des risques qui nécessitent l'attention de la direction.
Cette analyse se fait généralement à l'aide d'une matrice des risques (voir figure n° 2), qui permet d'illustrer et de classer les risques qui doivent être gérés de façon prioritaire par la direction, et ce selon leur degré d'impact et leur probabilité de survenance.
Les risques doivent être classés de manière logique, du plus important (impact élevé et forte probabilité) au moins significatif (faible impact et faible probabilité), comme indiqué dans la matrice (DiNapoli, 2007).

Figure N°2: la matrice des risques



Source : adapté de Hightower (2009)

2.3. Evaluation du degré d'aversion au risque de l'organisation

Le degré d'aversion au risque d'une organisation équivaut au niveau de risque qu'elle peut supporter avant de considérer la nécessité d'agir (INTOSAI, 2004). L'identification du degré d'aversion au risque d'une organisation est une question d'ordre subjectif puisqu'elle dépend de la perception de chaque organisation de l'importance des risques qu'elle peut encourir.

Il s'avère indispensable de prendre en compte à la fois les risques inhérents et résiduels afin de déterminer le degré d'aversion au risque d'une organisation (INTOSAI, 2004) :

- Le risque inhérent: est le risque qui se présente à une organisation lorsqu'elle ne mène aucune activité visant minimiser la possibilité de survenance ou l'impact du risque. (IFACI, 2013).
- Le risque résiduel : est le risque qui persiste après la mise en place par une organisation des actions ayant pour but de minimiser la possibilité de survenance ou l'impact du risque. (IFACI, 2013).

Chaque organisation devrait être en mesure de prendre des décisions pour répondre aux risques en parallèle à l'identification du degré de risque tolérable (INTOSAI, 2004).

2.4. Réponses à apporter aux risques

Les actions décrites ci-dessus permettront à l'organisation de dresser un profil propre à chaque risque (INTOSAI, 2004), ce qui aidera l'organisation à apporter des réponses pour chaque type de risques et déterminer ainsi, les risques qui sont acceptables et ceux qui ne le sont pas.

En tenant compte de l'impact et de la probabilité de survenance, l'organisation peut alors choisir de :

→ Accepter le risque : c'est-à-dire assumer le risque au sein de l'organisation (Hightower, 2009), et de ne pas établir des activités de contrôle concernant celui-ci (DiNapoli, 2007). Cette décision concerne les risques ayant une faible probabilité de survenance et un faible impact potentiel (Hightower, 2009 ; Bruwer, 2016).

→ Prévenir ou réduire le risque: c'est-à-dire établir des activités de contrôle pour anticiper le risque ou le réduire à un niveau acceptable. Pour ce faire, la direction devrait répondre à une batterie de questions afin d'identifier les activités de contrôle les plus efficaces et efficientes à la gestion du risque en question (DiNapoli, 2007) :

- ***Quelle est la cause du risque?*** La direction devrait considérer la raison pour laquelle le risque existe afin d'identifier toutes les activités de contrôle possibles qui pourraient prévenir ou réduire le risque.
- ***Quel est le coût du contrôle par rapport au coût de l'événement défavorable?*** La direction devrait comparer le coût engendré par le risque avec le coût de la

réalisation des différentes activités de contrôle, puis sélectionner le choix le plus rentable.

- ***Quelle est la priorité de ce risque?*** La direction devrait utiliser la liste de risques prioritaires pour décider comment répartir les ressources entre les diverses activités de contrôle destinées à réduire les risques. Plus la priorité est élevée, plus les ressources allouées aux activités de contrôle destinées à réduire le risque.

Cette décision peut concerner les risques ayant une forte probabilité de survenance avec un impact potentiel faible (Hightower, 2009 ; Bruwer, 2016).

→ Éviter le risque: certains risques ne peuvent être gérés qu'à travers leur élimination de la structure de l'organisation, en mettant à terme l'activité qui y est reliée. Cela peut se traduire dans l'organisation par l'abandon d'une gamme de produits, la renonciation à l'expansion vers une zone géographique donnée, ou la cession d'une division (COSO, 2013). Cependant, la décision d'éviter le risque peut être souvent facilement adoptée par une entreprise agissant au secteur privé, nonobstant, elle reste difficile à appliquer au secteur public où une activité à forts risques ne peut être abandonnée car elle relève de l'intérêt public (INTOSAI, 2004).

La décision de prévenir ou réduire le risque concerne principalement les risques ayant une forte probabilité de survenance et un impact potentiel élevé (Hightower, 2009 ; Bruwer, 2016).

→ Transférer le risque : consiste à prendre des mesures de transfert ou de partage des risques au sein de l'organisation, ou à rémunérer un tiers pour qu'il assume le risque autrement, à travers une assurance contre les pertes, à titre d'exemple, ou par le biais de clauses contractuelles (INTOSAI, 2004). Cette mesure concerne les risques caractérisés par une faible probabilité de survenance et un impact potentiel élevé (Hightower, 2009 ; Bruwer, 2016).

3. Considération du potentiel de fraude

La direction doit tenir compte du potentiel de fraude dans l'évaluation des risques, et ce afin d'atteindre les objectifs de l'organisation.

En effet, la fraude est un acte accompli dans l'illégalité dans le but de tromper délibérément, à soutirer de l'argent contre la volonté de quelqu'un ou à falsifier intentionnellement un document et porter atteinte aux droits ou aux intérêts d'autrui (Le Maux et al., 2013). L'ACFE (2012) définit la fraude comme étant « *l'utilisation par une personne de son activité professionnelle pour s'enrichir personnellement par le détournement volontaire des ressources ou des actifs de son employeur* ».

Ceci étant dit, la fraude se distingue par la présence de trois éléments qui la caractérisent : un élément intentionnel, une volonté de dissimulation et un mode opératoire (Ouashil & Ouhadi, 2019).

La littérature académique et professionnelle, notamment Wells (2007), distingue trois catégories de fraude au sein d'une organisation à savoir, la publication d'états financiers falsifiés, le détournement d'actifs et la corruption (Le Maux et al., 2013 ; COSO, 2013) :

- → ***La fraude relative aux états financiers*** : est un acte illégal basé sur un traitement comptable non conforme et intentionnel, et qui consiste à duper les utilisateurs des états financiers et les induire en erreur (principalement les créanciers et les actionnaires). Elle peut prendre la forme d'une modification des documents comptables, d'une déclaration inexacte des transactions, ou d'une mauvaise application intentionnelle des principes comptables.
- → ***Le détournement d'actifs*** : est un acte frauduleux qui consiste pour une personne à qui l'on a confié la gestion des actifs ou des fonds d'une organisation, à s'approprier, voler, céder ou utiliser ces biens pour son propre intérêt. Cela peut inclure le vol de biens, des propriétés intellectuelles, le détournement de reçus, le blanchiment d'argent ou des paiements frauduleux.
- → ***La corruption*** : est une pratique illicite consistant à user abusivement d'un pouvoir dans le dessein de réaliser des fins personnelles en échange d'une faveur, d'une somme d'argent ou d'autres avantages.

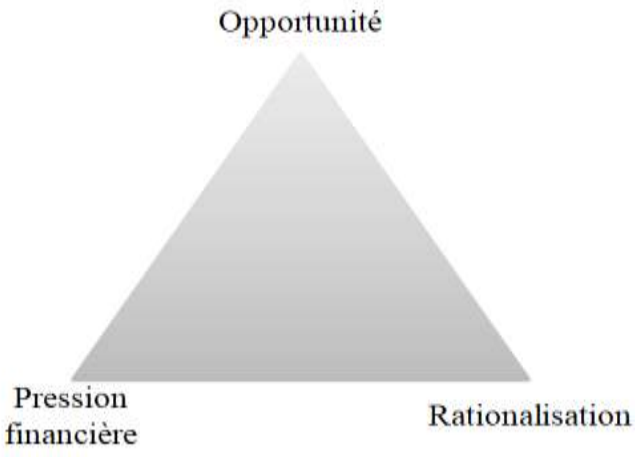
La théorie classique de la fraude explique depuis longtemps les raisons pour lesquelles une personne est impliquée dans une fraude financière ou tout autre type de fraude. Cette théorie décrit les motivations qui poussent les individus à s'impliquer dans la fraude, et ce à travers une illustration appelée « *le triangle de la fraude* » (voir figure n° 3), élaboré par Cressey (1950) et qui est composé de la pression, l'opportunité et la rationalisation :

→ ***La pression*** : désigne le sentiment ressenti par un individu suite à une très forte pression financière, qu'il ne peut pas partager ou faire subir à son entourage, et qui créé en lui la motivation de la fraude, cherchant ainsi à résoudre un problème d'ordre financier.

→ ***L'opportunité*** : désigne l'opportunité identifiée par un individu, qui lui permet de réaliser une action frauduleuse. L'opportunité se manifeste de deux façons : la première est due à la connaissance approfondie de l'organisation par l'individu, qui lui permet de déceler l'existence d'une faille dans le système de contrôle, et la seconde est due au sentiment du fraudeur que son acte ne pourra pas être détecté (Le Maux et al., 2013).

→ ***La rationalisation*** : désigne le processus par lequel le fraudeur réalise son acte tout en restant dans sa zone de confort moral, et arrive à se convaincre que ses actes ne peuvent pas être qualifiés d'actes illégaux. Cette rationalisation peut découler du fait que l'individu considère les ressources faisant objet de fraude comme un emprunt, et possède pleinement l'intention de les rembourser ultérieurement, ou l'individu croit que quelque chose lui est dû (ressources objets de fraude) en raison de l'insatisfaction au travail (salaire, environnement de travail, traitement par les managers), ou bien simplement l'individu ne se rend pas compte ou ne se soucie pas des conséquences de ses actes frauduleux (COSO, 2013).

Figure N°3: le triangle de la fraude



Source : Cressey (1950)

Les énoncés sur le contrôle interne, notamment le référentiel COSO (2013), déclarent que la direction devrait considérer la fraude comme étant un type de risque qu'elle doit prendre en compte dans son processus d'évaluation des risques. Et qu'elle doit analyser et répondre aux risques de fraude identifiés afin qu'ils soient efficacement atténués, et ce à travers l'adoption du même processus utilisé pour l'ensemble des risques analysés.

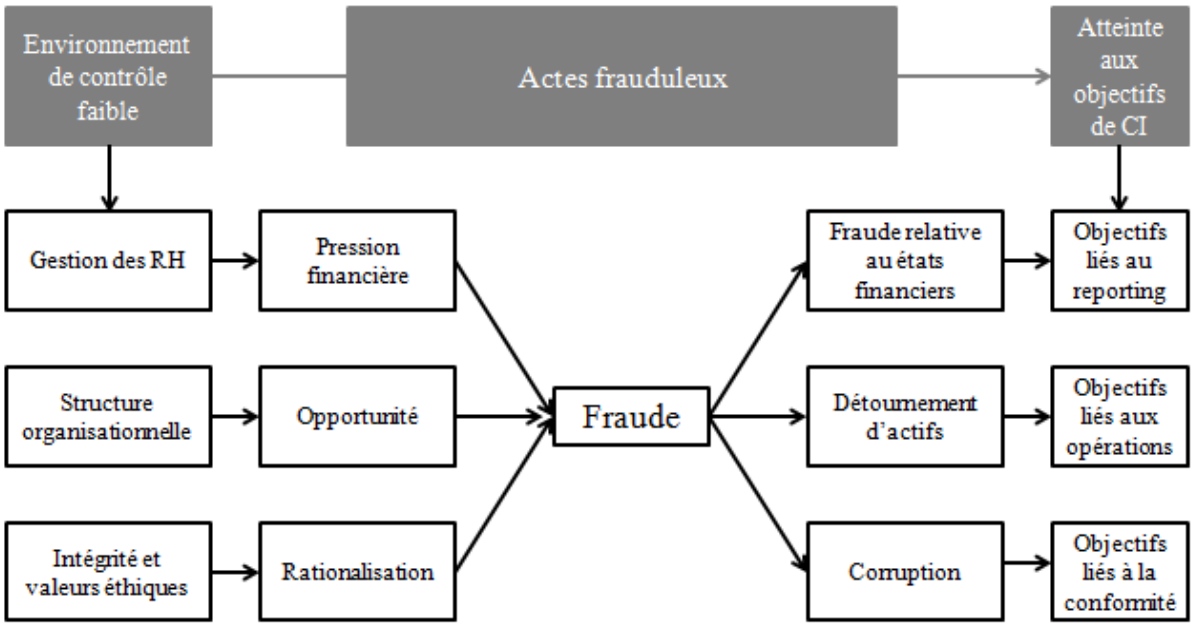
Néanmoins, Hightower (2009) signale qu'il ne faut pas confondre entre un risque et une fraude. Elle déclare qu'il est plus difficile d'atténuer les fraudes que d'atténuer les risques, du fait que l'organisation peut difficilement avoir un effet sur la motivation d'un individu pour commettre une fraude. Par contre, selon la même auteure, l'opportunité de fraude est un champ plus facile à traiter par l'organisation, à travers la mise en place de celle-ci des systèmes de contrôle interne efficaces. Elle ajoute que l'intégrité des individus peut éventuellement être soutenue et renforcée grâce à des programmes de formation et de sensibilisation pour agir sur le point de rationalisation.

Nous constatons alors qu'il existe une relation causale entre l'environnement de contrôle, la fraude et les objectifs de contrôle interne. En effet, l'existence d'un environnement de contrôle faible favorise l'existence éventuelle d'une fraude, ce qui peut nuire aux objectifs de contrôle interne. Ceci étant dit, nous avions énoncé précédemment que l'environnement de contrôle constitue les bases fondatrices d'un bon système de contrôle interne, à défaut d'un environnement de contrôle sain, le système global de contrôle interne est voué à l'échec.

Cependant, le dysfonctionnement d'un ou de plusieurs éléments qui constituent l'environnement de contrôle d'une organisation présente un champ propice à l'apparition des éléments favorisant la réalisation des actions frauduleuses.

En se basant sur le triangle de Cressey (1950) et sur les travaux du référentiel COSO (2013), nous avons élaboré un modèle qui illustre la relation causale entre la fraude et le contrôle interne:

Figure N°4: modèle illustrant la relation causale entre l'environnement de contrôle, la fraude et les objectifs de contrôle interne.



Source : réalisé par nos propres soins

Elément de l'environnement de contrôle, une gestion des ressources humaines inadéquate, qui n'adopte pas une équité salariale en ce qui concerne sa politique de rémunération, ou qui ne respecte pas les performances de son personnel en pratiquant la rétribution méritée pour les efforts fournis, ou qui pratique un niveau des salaires inférieur par rapport à la concurrence, a tendance à créer un sentiment d'injustice au niveau de son personnel, ce qui pourra pousser ce dernier à commettre des actes frauduleux.

Une gestion des ressources humaines qui n'encourage pas les employés à travers un système de primes, de récompenses ou de gratifications pour récompenser leur rendement ou les heures supplémentaires travaillées, et qui ne les fait pas bénéficier des avantages complémentaires permettra la naissance d'un sentiment d'insatisfaction au niveau de l'ensemble du personnel d'une organisation.

En effet, les travaux d'Adams (1963) dans le domaine de la psychologie sociale ont démontré que les salariés comparent leur contribution à la rétribution reçue en contrepartie. Les employés confrontent le ratio contribution/rémunération à celui d'autres salariés membres de

la même organisation ou d'organisations concurrentes (Sachet-Milliat, 2010). Adams montre que les employés estimant n'être pas récompensés à leur juste valeur vont ressentir un état de tension psychologique qui va impacter de façon négative leur motivation et engendrer des attitudes visant à rétablir la justice. Les employés vont essayer d'agir sur la diminution de leur contribution à travers la réduction des heures de travail ou à travers l'absentéisme. Soit d'œuvrer sur le rehaussement de leur rémunération à travers des actes licites, notamment la demande d'augmentation du salaire ou par le biais d'actes illicites comme le détournement frauduleux des actifs.

De même, une politique des ressources humaines qui n'assure pas à ses employés un environnement de travail adéquat et sain, et qui ne leur garantit pas un système de protection sociale qui couvre les accidents de travail et les cas de maladie ou de décès, développera une sensation d'insécurité au sein de l'organisation où ils travaillent.

Donc nous pouvons dire qu'une organisation qui possède une politique de gestion des ressources humaines inefficace, qui pousse ses employés à sentir l'insatisfaction, l'injustice ou l'insécurité, favorisera à travers ses actions, la naissance d'une pression financière au niveau de ses employés, face à des situations où ces derniers confrontent des problèmes d'ordres financiers, médicaux ou sociaux, ce qui va créer en eux la motivation de commettre un acte frauduleux.

L'opportunité de fraude pourra avoir plusieurs origines, comme par exemple, une structure organisationnelle inadéquate, caractérisée par l'instabilité ou la complexité. Ceci dit, une structure qui ne soutient pas la délégation de pouvoir, où la répartition des tâches professionnelles est inégale et qui reflète une inadéquation entre le poste de responsabilité et le profil de compétence exigé, pourra engendrer des relations conflictuelles et un environnement de travail instable, ce qui causera un taux élevé de turnover et des failles de fonctionnement, créant ainsi une opportunité adéquate pour commettre une fraude.

La rationalisation est le processus par lequel le fraudeur justifie ses actes à ses propres yeux et à ceux d'autrui, et arrive à se convaincre qu'il ne se considère pas coupable. La rationalisation est donc une question subjective, qui diffère d'une personne à une autre selon ses traits de caractère, ses principes moraux et s'il est susceptible ou pas d'adopter des comportements non éthiques.

Le rôle de l'organisation réside alors d'intégrer les critères éthiques dans ses procédures d'embauche pour recruter des employés intègres, et de choisir les personnes les plus honnêtes.

Bien entendu, l'évaluation de l'éthique des candidats doit être effectuée dans le respect total de la législation en matière de recrutement, à défaut, l'organisation pourra difficilement solliciter de ses employés un comportement moral si elle-même ne respecte pas des normes éthiques dans sa politique de gestion des ressources humaines (Sachet-Milliat, 2010).

L'organisation doit également veiller à sensibiliser son personnel à l'éthique et institutionnaliser les valeurs éthiques en créant une référence culturelle commune, sans oublier, l'importance d'adopter une politique de rémunération équitable comme nous avons cité précédemment.

La fraude, telle que démontrée dans le modèle COSO (2013) peut se manifester sous 3 formes : la fraude relative aux états financiers, le détournement d'actifs et la corruption. Chacune de ces trois manifestations de fraude porte une atteinte aux objectifs de contrôle interne en absence de mesures d'identification, de détection et de prévention des risques relatifs aux fraudes.

La fraude relative aux états financiers est une manipulation intentionnelle et non conforme des états financiers dans le but de tromper les acteurs concernés par ces-dits rapports. De ce fait, cette falsification représente une atteinte aux objectifs de reporting énoncés par le contrôle interne, qui consistent à garantir la fiabilité des états financiers. Le détournement d'actifs empêche la réalisation des objectifs liés aux opérations, puisque tout acte de maniement, de vol, de cession ou d'utilisation illégale d'un des biens de l'organisation représente une violation à l'objectif de sauvegarde des actifs et du patrimoine de l'organisation.

De même, la corruption est un acte illégal puni par la loi, et qui symbolise une transgression des lois et règlements en vigueur, portant ainsi atteinte aux objectifs de conformité, qui visent le respect de l'organisation et de son personnel des lois et des règlementations.

4. Identification et évaluation des changements significatifs

Les conditions économiques, industrielles, réglementaires et opérationnelles ne cessent de changer, et les organisations sont amenées à accompagner ces changements de manière continue.

Le changement, de par sa nature, crée un certain degré de risque (GFOA[2], 2007). Dès lors, la mise en place par les organisations, des mécanismes pour identifier et gérer les risques particuliers associés au changement s'avère nécessaire (Frazer, 2012).

[2] GFOA acronyme de « Government Finance Officers Association » qui est une association professionnelle présente aux Etats-unis et au Canada.

L'organisation peut être face à des changements d'ordre externes et interne (GFOA, 2007 ; COSO, 2013). Les changements externes peuvent être relatifs au changement de l'environnement économique, social et politique, des nouvelles dispositions légales et règlementaires, une modification de la fiscalité, des catastrophes naturelles, etc. et Les changements d'ordre internes peuvent se manifester à la suite d'un changement au niveau de la direction et des postes de responsabilité ou au niveau du personnel, un changement de structure, etc.

Ceci étant dit, la direction doit être en veille continue par rapports aux changements externes et internes qui présentent une source de risque potentiel, et identifier, analyser et réagir aux différents changements pouvant avoir une incidence sur le système de contrôle interne de l'organisation.

Un contrôle interne efficace dans certaines conditions peut ne le pas être nécessairement lorsque ces conditions changent de manière significative (COSO, 2013). À cet effet, le processus d'identification et d'analyse du changement devrait être parallèle ou faire partie du processus régulier d'évaluation des risques de l'organisation. Cela implique d'identifier et communiquer les changements pouvant affecter les objectifs de l'organisation et détecter les risques qui leur sont associés. Ces changements doivent être analysés à la fois pour leur effet immédiat et pour leur impact futur. La direction déterminerait alors toute modification nécessaire au processus de contrôle interne pour s'adapter à ces changements.

Conclusion

Aucune organisation ne peut prétendre être à l'abri des risques, du fait que ce dernier revêt un caractère inattendu et imprévisible. Cependant, les organisations peuvent contrecarrer les risques à travers un bon système de contrôle interne. L'évaluation des risques constitue, avec les autres composantes, les bases d'un contrôle interne solide et efficace, ayant pour but d'aider les organisations à atteindre leurs objectifs.

Grâce au processus l'identification, d'analyse et de choix des réponses à adopter face aux différents types de risques, l'évaluation des risques permet à chaque organisation de détecter, d'anticiper et éviter les risques.

À travers le processus d'évaluation des risques, le contrôle interne ne néglige pas la potentialité d'existence de fraude, qu'il faut comme tout type de risque, identifier et analyser. Néanmoins, le processus d'évaluation du risque de fraude ne dispense pas les organisations de

veiller à construire un environnement de contrôle solide. En effet, un environnement de contrôle basé sur une politique de ressources humaines équitable, un personnel qualifié et intègre et une philosophie qui promeut les valeurs d'éthique permettra sans doute d'agir positivement sur les sources de fraude, et donc minimiser la survenance des actes frauduleux pouvant mettre en enjeux les objectifs de contrôle interne.

Puisque les organisations évoluent dans un environnement qui change constamment, l'évaluation des risques prend en compte le facteur du changement comme source de risque que chaque organisation ne doit pas négliger.

Suite à l'étape d'évaluation des risques, la direction peut alors déterminer les actions à entreprendre face à ces derniers et développer les activités de contrôle associées : L'évaluation des risques constitue alors la base de la conception des activités de contrôle- qui constituent la troisième composante du contrôle interne- pour atténuer ces risques.

Néanmoins, certains auteurs ont remarqué l'insuffisance du processus d'évaluation des risques et ont appelé à une plus grande intégration des concepts de gestion des risques au sein des organisations. En se penchent vers une optique plus approfondie du management des risques, le COSO propose un nouveau cadre de référence orienté risques de l'entreprise « COSO 2 Entreprise Risk Management », qui inclut les éléments du COSO 1 et qui évoque de nouvelles notions telles que le « Risk Appetite » (appétence aux risques) et le « Risk Tolerance » (tolérance aux risques ». Nonobstant, nous nous interrogeons : Quels sont les apports du COSO 2 par rapport au COSO 1 en matière de gestion des risques ? est ce que l'adoption de l'ERM par les organisations s'avère incontournable pour contrecarrer les risques ? Et dans quelle mesure l'implémentation du contrôle interne et de l'ERM contribue-t-elle dans la gouvernance des organisations ?

BIBLIOGRAPHIE

- ACFE (2012). *Report to the nation on occupational fraud and abuse*.
- Adams, J. (1963) « towards an understanding of inequity » journal of abnormal and social psychology, vol 67, n°5, p.422-426.
- AFNOR, (2010) « Management du risque - Principes et lignes directrices », NF, ISO 31000, Indice de classement : X50-254
- Archbold, C.A. (2005) « Managing the bottom line: risk management in policing ». Policing: An International Journal of Police Strategies & Management.
- Aven, T. (2011) On the new ISO guide on risk management terminology. Reliability Engineering and System Safety.
- Aven, T. Renn, O. (2009). "On risk defined as an event where the outcome is uncertain". Journal of Risk Research.
- Bhimani, A. (2009) "Risk management, corporate governance and management accounting: Emerging interdependencies". Management Accounting Research.
- Bruwer, J.P. (2016) "the relationship(s) between the managerial conduct and the internal control activities of South African fast moving consumer goods SMMES" CAPE PENINSULA UNIVERSITY OF TECHNOLOGY.
- Buys, J.P. (2012) "A conceptual framework for determining sustainability of SMMEs in Lesedi." Unpublished MBA dissertation, North West University, Potchefstroom, South Africa.
- Caeymaex, F. (2007) « Risquer, gérer, sécuriser : techniques politiques de la modernité ? », Techniques et philosophies des risques, Paris, Vrin, pp. 111-122.
- COSO. (1992). Internal control – integrated framework. Jersey City, NJ: Committee of Sponsoring Organizations of the Treadway Commission.
- COSO. (2013). Internal control – integrated framework: executive summary.
- Cressey, D.R. (1950) "The criminal violation of financial trust", American Sociological Review, vol. 15, n° 6, p. 738-743.
- DiNapoli, T.P. (2007) "Standards for Internal Control in New York State Government"
- Frazer, L. (2012) "The effect of internal control on the operating activities of small restaurants". Journal of Business & Economics Research.
- Grebe, G.P.M. (2014) The management of fraud risk in South African private hospitals. Unpublished (Business Management) dissertation, University of South Africa, Pretoria.

- Hadji Rezai, S. (2017) Méthode d'évaluation de l'impact des composants de construction sur la performance globale (énergétique environnementale, économique et sociale) d'un bâtiment tout au long de son cycle de vie. Génie civil. Université de La Rochelle.
- Hightower, R. (2009) "Internal Controls Policies and Procedures", John Wiley & Sons, Inc. États-Unis.
- Hillson, D. (2002) «Extending the risk process to manage opportunities.» International Journal of Project Management.
- IFACI (2013) « La cartographie des risques », cahier de la recherche, 2ème édition.
- INTOSAI (2004) « Lignes directrices sur les normes de contrôle interne à promouvoir dans le secteur public ».
- ISO (2002) Risk Management Vocabulary. ISO/IEC Guide 73.
- Kaplan, S. Garrick, B.J. (1981) « On the quantitative definition of risk: Risk Analysis».
- Kermisch, C. (2012) « Vers une définition multidimensionnelle du risque », Vertigo, volume 12 n°2.
- Kommunuri, J., Jandug, L. & Vesty, G. (2014). Risk management, board effectiveness and firm value: evidence from S&P/ASX200 companies. In Uneo, S. & Nitirojntanad, K. (eds). Proceedings of the 10th Asia-Pacific Management Accounting Association Annual Conference (APMAA 2014): Management Accounting in a Global, Dynamic Environment: Challenges and Opportunities, Bangkok, Thailand, 27–30 October. Bangkok, Asia-Pacific Management Accounting Association.
- Kumamoto, H. Henley, E. (1996) Probabilistic Risk Assessment and Management for Engineers and Scientists.
- Le Maux, J.,Smaili, N. et Ben Amar, W. (2013) «DE LA FRAUDE EN GESTION À LA GESTION DE LA FRAUDE Une revue de la littérature. », Revue française de gestion, N° 231, pages 73 à 85.
- Le Ray, J. (2012) « Premiers pas dans le management du risque, Techniques de l'ingénieur »
- Luís, A., Lickorish, F. & Pollard, S. (2015) « Assessing interdependent operational, tactical and strategic risks for improved utility master plans». Water Research.

- Nissanke, N. & Dammag, H. (2002) Design for safety in Safecharts with risk ordering of states. Safety Science.
- November, V. & Leanza, Y. (2015) Risk, disaster and crisis reduction: mobilizing, collecting and sharing information.
- Ouashil M. & Ouhadi S. (2019) « Le contrôle interne face à l'émergence de nouvelles formes des risques : cas de la fraude » Revue Internationale des Sciences de Gestion « Numéro 3 : Avril 2019 / Volume 2 : numéro 2 » p : 805 - 819
- Oseifuah, E K., Gyekye, A B., (2013) «Internal control in small and microenterprises in the VHEMBE district, LIMPOPO PROVINCE, SOUTH AFRICA» , European Scientific Journal , edition vol.9, No.4.
- Prinsloo, S., Walker, C., Botha, L., Bruwer, J-P. & Smit, Y. (2015) « The influence of combined assurance initiatives on the efficiency of risk management in retail small and very small enterprises in Bellville, South Africa». Expert Journal of Business and Management.
- Remenyi, D. & Heafield, A. (1996) Business process re-engineering: some aspects of how to evaluate and manage the risk exposure. International Journal of Project Management.
- Ritchie, B. & Brindley, C. (2007) Supply chain risk management and performance: a guiding framework for future development. International Journal of Operations & Production Management.
- Rosa, E. (1998) Meta theoretical foundations for post-normal risk. Journal of Risk Research.
- Sachet-Milliat, A. (2010) « la prévention de fraude des salariés par des pratiques éthiques de management ». Revue des directeurs sécurité d'entreprise / hors série, pages 75 à 85.
- Sanne, J.M. (2008) «Incident reporting or storytelling? Competing schemes in a safety-ritical and hazardous work setting». Safety Science.
- Schwartz, M.S., Dunfee, T.W. & Kline, M.J. (2005) Tone at the top: an ethics code for directors? Journal of Business Ethics.
- Sin, I. & Ng, K. (2013) The evolving building blocks of enterprise resilience: ensnaring the interplays to take the helm. Journal of Applied Business and Management Studies.

- Smit, Y. (2012) A structured approach to risk management for South African SMEs. Unpublished DTech: Internal Auditing thesis, Cape Peninsula University of Technology, Cape Town, South Africa.
- Spekman, R.E. & Davis, E.W. (2004) «Risky business: expanding the discussion on risk and the extended enterprise». International Journal of Physical Distribution and Materials Management.
- Sudsomboon, S. & Ussahawanitchakit, P. (2009) « Professional audit competencies: the effects On Thai's CPAS audit quality, reputation, and success». Review of Business Research, 66 – 85.
- Tchankova, L. (2002) Risk identification – basic stage in risk management. Environmental Management and Health.
- Theofanis, K., Drogalas, G. & Giovanis, N. (2011) «Evaluation of the effectiveness of internal audit in Greek Hotel Business. » International Journal of Economic Sciences and Applied Research, 19-34.
- Vatsa, K.S. (2004) «Risk, vulnerability, and asset-based approach to disaster risk management. » International Journal of Sociology and Social Policy.
- Weber, O., Scholz, R.W. & Michalik, G. (2010) «Incorporating sustainability criteria into credit risk management. » Business Strategy and the Environment.
- Wells J. (2007). « Corporate fraud handbook: Prevention and detection. » John Wiley & Sons, Inc., États-Unis.
- Wood, O.G. Jr. (1964). «Evolution of the concept of risk». Journal of Risk and Insurance.