UNIVERSITE CATHOLIQUE DE LOUVAIN

LOUVAIN SCHOOL OF MANAGEMENT

Stratégie d'implémentation d'un ERM au sein de l'Université catholique de Louvain : Utopie ou Réalité ?

CONFIDENTIEL

Promoteur : Loïc Decaux
Co-Promoteur : Gerrit Sarens

Mémoire-projet présenté par
François-Xavier Van Vlasselaere

en vue de l'obtention du titre de
Master en ingénieur de gestion

ANNEE ACADEMIQUE 2014-2015

Je tiens à exprimer ma gratitude à Monsieur le Professeur Gerris Sarens et à Monsieur Loïc Decaux pour toute l'aide apportée à la réalisation de ce mémoire. Leur disponibilité ne fut jamais prise en défaut. Je remercie également l'ensemble du corps académique, scientifique et administratif de la *Louvain School of Management* et de la Faculté des Sciences Economiques, Sociales et Politiques pour toute la formation antérieure sans laquelle ce mémoire n'aurait pu aboutir. Que toutes les personnes qui m'ont aidé pour ce mémoire soient également remerciées.

Table des Matières

Introduction

"C'est quand la mer se retire qu'on voit ceux qui se baignent nus."(Warren Buffet). L'Université catholique de Louvain (UCL) est-elle préparée à un tel reflux?

L'UCL s'est développée autour d'une gestion traditionnelle. Par contre les exigences du monde moderne s'imposent à elle. La mondialisation et la globalisation de l'économie ont pris de plus en plus d'ampleur (Adda, 2007). Le monde universitaire en est également affecté. On peut citer pour exemples les classements internationaux et les échanges interuniversitaires. Face à ce défi, de nouvelles méthodes de gestion ont émergé. Sous la pression des pouvoirs publics, les universités anglo-saxonnes ont développé en leur sein un processus rationnel de gestion des risques.

Dans la mesure où cette évolution anglo-saxonne est très peu présente en Europe Continentale, il nous est apparu judicieux d'examiner les conditions de possibilité d'implémentation d'une gestion moderne des risques à l'UCL, université dans laquelle ma formation universitaire fut effectuée. Ce mémoire s'adresse avant tout aux autorités de l'UCL afin de les éclairer sur l'intérêt, voire la valeur ajoutée, qu'un tel projet d'implémentation pourrait permettre d'engranger.

L'Université catholique de Louvain est une université belge privée et subventionnée évoluant en Fédération Wallonie-Bruxelles. Le financement des universités francophones est basé sur une enveloppe fermée qui n'a pas évolué depuis 1996 malgré l'augmentation de plus de 20% du nombre d'étudiants (Fédération Wallonie-Bruxelles, 2014). Dans cette perspective qui lui est imposée, l'UCL est sensibilisée dans l'optimalisation de ses ressources afin de faire face à ses objectifs qui sont l'enseignement, la recherche et les services à la société [1].

Dans la situation actuelle, les différents risques présents au sein de l'institution sont gérés en silos organisationnels et en bon père de famille. Cette façon de procéder ne permet pas au management d'avoir une image globale de la gestion et encore moins de l'optimaliser. Une

[1] Déc. Comm. fr. du 31 mars 2004 définissant les missions de l'enseignement supérieur en Communauté française, art.3, *M.B.* 2014

étude préparatoire sur la gestion des risques a été initiée dès 2008 et est toujours en cours. Cette recherche a pris son origine au départ de la constatation que les polices d'assurance souscrites par l'université ne sont pas adaptées de manière efficiente aux risques à couvrir. Cette étude a débouché notamment sur un document de travail confidentiel relatif à la *"Gestion des risques – Etude exploratoire : risques perçus par les membres du CODIR"* (Rombouts 2013).

Le mémoire s'inscrit dans cette problématique et essaye d'examiner si une implémentation d'un *Entreprise Risk Management* (ERM) est possible au sein de l'UCL. Il s'interroge pour savoir s'il s'agit d' *"une utopie ou* (d') *une réalité ?"*. Nous remarquerons que la réponse est beaucoup moins catégorique qu'il n'y paraît. En effet, une implémentation d'un ERM dès à présent serait prématurée mais, après une phase complémentaire d'investigation et d'adaptation de l'organisation aux conditions d'une bonne implémentation, celle-ci devrait pouvoir être envisagée si les hypothèses de changements nécessaires sont réalisées.

Nous aurons dans un premier temps à analyser la théorie relative à l'implémentation d'un ERM dans une organisation en général. La principale source méthodologique se trouve dans le guide du *Committee of Sponsoring Organizations of the Treadway Commission* (COSO 2004). Ce guide a servi également de référentiel à l'étude exploratoire. L'analyse théorique sera complétée par des publications, des reportings et des articles scientifiques. Une attention toute particulière sera portée sur les implémentations d'un processus d'ERM effectuées dans les universités étrangères.

Dans un second temps, le travail sera focalisé sur les particularités de l'UCL. Les différents documents émanants de celle-ci ont été examinés et des interviews de certains responsables du comité de direction (CODIR) seront effectuées.

Ensuite, une mise en parallèle de la théorie générale et du cas pratique de l'UCL permettra de déboucher sur l'examen de la possibilité d'implémenter un ERM au sein de l'institution ainsi que sur des conseils au management d'une politique future.

Partie I: Revue de littérature sur la gestion des risques et de l'ERM

1 Avènement de l'Entreprise Risk Management

Le concept de risque est devenu une notion centrale de la gouvernance des organisations (Spira & Page, 2003). Selon Beasley, Clune & Hermanson (2005), la gestion du risque est un nouveau modèle permettant aux organisations de gérer leurs risques et d'améliorer la bonne gouvernance. De nombreux auteurs (Jorion, 2008 ; Stulz, 2008; Baker, 2009 ; Lenz & Sarens, 2012 ; Landsittel & Rittenberg, 2010) ont démontré que la crise bancaire et financière de l'automne 2008 était en partie due à une mauvaise gestion des risques. Celle-ci a contribué à augmenter les tensions financières (FSB, 2009). Baker (2009) dénonce une mauvaise évaluation et identification des risques dans le chef des entreprises. Selon Arena, Arnaboldi et Azzone (2010), l'intérêt dans la gestion du risque et, plus particulièrement, dans les ERM a considérablement augmenté au cours des dernières années.

L'environnement concurrentiel dans lequel les organisations se meuvent est à la base de nouveaux risques. On peut citer les nouvelles législations, les avancées technologiques ou encore le contexte de la mondialisation (KPMG, 2007). Une gestion appropriée et méthodique des risques peut aider les organisations dans ces nouveaux défis. Selon Walker, Shenkir et Barton (2002), la gestion des risques est une demande des différentes parties prenantes des organisations pour améliorer le contrôle des risques clés et afin de conserver et d'améliorer leurs investissements.

Bien que la structure, l'objectif et le mode de fonctionnement des différentes organisations peuvent varier, la gestion des risques à proprement dit se base sur les mêmes fondements théoriques (COSO, 2004 ; ISO , 2009 ; ASX Corporate Governance Council ; 2007). Dans la pratique, certains éléments de la gestion peuvent être accentués en fonction des objectifs à atteindre. Ces guides de bonne gouvernance, impliquant des changements de régulations, ont contribué à l'augmentation de l'intérêt pour la gestion du risque (Kleffner, Lee & McGannon, 2003).

La gestion des risques possède certaines caractéristiques communes aux organisations, dont l'étude approfondie est nécessaire pour réussir une implémentation. Une bonne implémentation de l'ERM doit fournir à l'entreprise un avantage concurrentiel (Stroh, 2005). Il convient d'analyser chaque composante en profondeur pour maximiser les chances de succès de l'ERM. Bien que la gestion des risques fasse l'objet d'un travail collectif, certaines personnes auront un rôle plus déterminant dans le processus (Power, 2007). En fonction de l'implémentation, cette gestion s'articulera autour de fonctions, telles que celles de gestionnaire du risque ou de l'auditeur interne.

Le principal référentiel pris en compte pour l'analyse est le COSO. Cette organisation virtuelle est sponsorisée par cinq organisations, à savoir l'*American Accounting Association*, l'*American Institute of Certified Public Accountants*, la *Financial Executive International*, *The Institute of Internal Auditors* et l'*The Institute of Management Accountants*. L'influence du COSO s'étend sur les régulateurs, les firmes de consultance, les organisations privées et la communauté académique de manière internationnale (Landsittel & Rittenberg, 2010). Le COSO a adopté en 2008 une définition de ses objectifs. Ce dernier tente de *"fournir aux leaders une réflexion par des conseils et des guides sur l'Entreprise Risk Management, le contrôle interne et la prévention de la fraude visant à améliorer les performances de l'organisation et la gouvernance et de réduire l'étendue de la fraude dans les organisations."* (Landsittel & Rittenberg, 2010, p.457, traduction). Le guide de référence en rapport avec la gestion des risques est le suivant : *Entreprise Risk Management-Integrated Framework* publié en 2004.

2 Définition du risque

Afin de pouvoir appréhender la gestion des risques au sein des organisations, il faut au préalable définir ce qu'est un risque et quelle forme doit en revêtir la gestion. Selon Spira & Page (2003), la notion formelle de gestion des risques inhérente aux entreprises a évolué de nombreuses fois dans l'histoire, passant d'une obligation formelle à un outil d'aide au management de l'organisation. La gestion des risques doit être considérée comme un outil permettant d'identifier, de quantifier et d'objectiver les risques réels et potentiels d'une organisation. Cette approche en profondeur dans

l'analyse est nécessaire à sa réutilisation dans la stratégie de l'entreprise.

De nombreuses définitions du risque sont présentes dans la littérature (ISO, 2009 ; Sarbanes-Oxley Act [2], 2002 ; CERA, 2009). Nous pouvons baser notre analyse sur la définition donnée par L'*International Organization for Standardization* (ISO). Cette dernière définit le risque dans sa norme 73 comme étant : *"un effet incertain sur les objectifs, l'effet pouvant être positif, négatif ou une déviation de ce qui est espéré et que le risque est souvent décrit par un évènement, un changement de circonstances ou une conséquence."* (ISO, 2009, p 5.). Cette définition donnée par l'ISO est assez vague mais a l'avantage de ne pas omettre des risques potentiels. En effet, les entreprises font face à des risques multiples pouvant être internes et externes à l'organisation et certains d'entre eux sont une combinaison subtile de différents facteurs interagissant entre eux (FERMA, 2002). L'illustration 1 nous donne une représentation de l'interaction pouvant exister entre les différents risques présents dans une organisation.

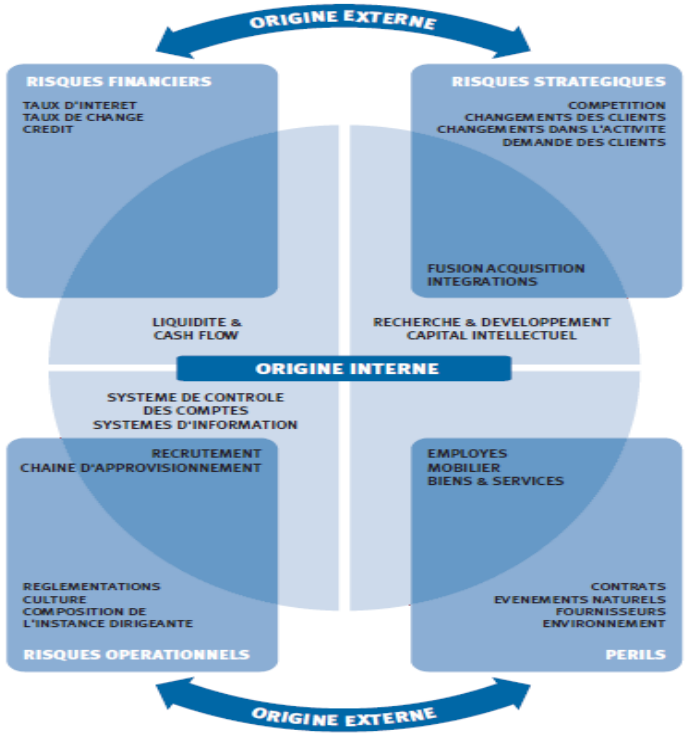


Figure 1: Typologie des risques internes et externes [3]

[2]Public Law 107-204 Sarbanes-Oxley Act of 2002 by the 107th Congress of the United States

[3](Source : FERMA *Cadre de référence de la gestion des risques* `http://www.ferma.eu/app/uploads/`

3 Gestion du risque

Nous allons, dans un premier temps, analyser les éléments centraux de l'ERM dans la prespective d'examiner par la suite si l'implémentation d'un tel ERM adapté à l'Université catholique de Louvain est possible. Une telle démarche n'a pas fréquemment été réalisée antérieurement.

3.1 Définition de la gestion du risque

Nous baserons notre analyse de la gestion du risque sur deux des nombreuses définitions existantes (Courtot, 1998 ; COSO 2004; CERA, 2009 ; NYSE Listing Standard, 2013). En effet, comme pour la définition du risque, de nombreuses définitions de la gestion de celui-ci sont également présentes dans la littérature. Courtot (1998) définit la gestion du risque comme étant un *"processus itératif appliqué tout au long d'un programme et qui regroupe les activités d'identification, d'estimation et de maîtrise des risques où l'estimation est vue comme le processus utilisé pour affecter des valeurs à la probabilité, à la détectabilité et aux conséquences d'un risque"* (Courtot, 1998,p. 38) . Cette première définition met en avant le coté procédural, bureaucratique et pragmatique de la gestion du risque. La gestion du risque est plus proche d'un outil scientifique que de celle de l'art, basée sur des méthodes ayant fait leurs preuves et conduisant à l'apparition de nouvelles fonctions dans l'organisation. Pesqueux (2011) donne une piste d'analyse générale pouvant être prise en compte dans la réalisation d'une étude des risques. Premièrement, il existe une phase d'analyse, qu'il dénomme la rationalité procédurale, permettant de classer les risques selon *"un ensemble cohérent de risques quant à leur nature et aux responsabilités associées à leur management"* (Courtot, 1998, p. 40). Deuxièmement, une phase de maîtrise permettant soit de lever, soit de transférer, soit d'atténuer le risque. Cette phase permettant également de voir quels risques sont acceptables pour l'organisation. Le processus de gestion des risques est passé d'un processus *"technico-scientifique"* de pure analyse à un concept plus vague qui tente de rassembler, sous un régime unique, de nombreux éléments disparates de l'entreprise (Spira & Page, 2003).

Le COSO a également donné une définition de l'ERM comme étant *"[...] un processus mis en œuvre par le conseil d'administration, la direction générale, le management et l'ensemble des*

2011/11/a-risk-management-standard-french-version.pdf)

collaborateurs de l'organisation. Il est pris en compte dans l'élaboration de la stratégie ainsi que dans toutes les activités de l'organisation. Il est conçu pour identifier les événements potentiels susceptibles d'affecter l'organisation et pour gérer les risques dans les limites de son appétence pour le risque. Il vise à fournir une assurance raisonnable quant à l'atteinte des objectifs de l'organisation" (COSO, 2004, p.3). Cette définition met l'accent sur l'approche descendante de la gestion du risque et sur la valeur ajoutée que cette gestion apporte à l'organisation pour atteindre ses objectifs.

Ce processus doit couvrir l'ensemble de l'organisation pour être efficace. Selon un rapport de l'IIAbel [4] en collaboration avec l'Institut des Reviseurs d'Entreprises (IRE) *"La coopération n'est possible que si les sociétés utilisent un cadre de gestion des risques couvrant l'ensemble de l'organisation et reconnaît ses avantages par rapport à des approches moins coordonnées de gestion des risques."* (2010, p. 34)

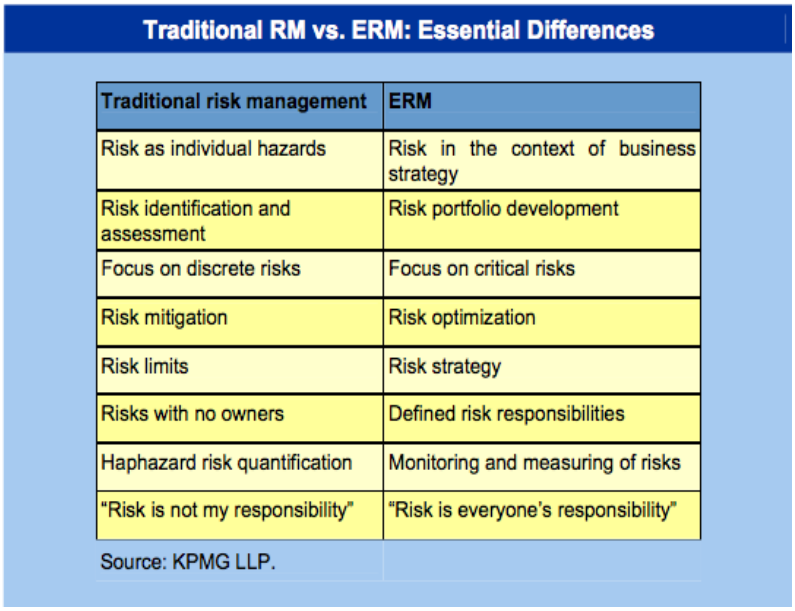
3.2 Composantes d'un ERM

Originellement, la gestion traditionnelle du risque [5] dans les organisations a été réalisée en silos (Christopher & Sarens, 2015 ; Yazid, Razali & Hussin, 2012), ce qui ne permettait pas de mettre en évidence l'interconnectivité des risques. Shaw (2005) rapporte que l'approche par silos rate deux aspects importants de l'ERM, à savoir la détermination de l'appétit du risque et l'identification des risques émergents. Hoffman (2002) montre qu'une analyse superficielle et trop simple des opérations mène à des pertes considérables pour les organisations. Contrairement à l'approche et al. , 2003). Selon Yazid et al. (2012), l'ERM permet d'intégrer et de coordonner les risques à l'intérieur d'une entreprise.

L'illustration 2 montre les différences fondamentales entre la gestion des risques par silos (TRM) et l'ERM.

[4] The Institute of Internal Auditors en Belgique

[5] Egalement appelée Traditional Risk Management



Traditional RM vs. ERM: Essential Differences

Traditional risk management	ERM
Risk as individual hazards	Risk in the context of business strategy
Risk identification and assessment	Risk portfolio development
Focus on discrete risks	Focus on critical risks
Risk mitigation	Risk optimization
Risk limits	Risk strategy
Risks with no owners	Defined risk responsibilities
Haphazard risk quantification	Monitoring and measuring of risks
"Risk is not my responsibility"	"Risk is everyone's responsibility"

Source: KPMG LLP.

Figure 2: Différences entre le TRM et l'ERM [6]

Selon le cadre référentiel du COSO, la gestion du risque au sein d'une organisation comprend plusieurs composantes interconnectées et intégrées au processus de management. Le processus n'est pas séquentiel mais multidirectionnel et itératif (COSO, 2004). En d'autres mots, chaque élément peut influencer potentiellement les autres éléments de manière directe. Selon Nelson et Ambrosini (2007), aucun aspect de l'ERM n'est plus important qu'un autre.

Le référentiel COSO synthétise les composantes de son ERM à travers le *Cube COSO* mettant en avant les différentes composantes critiques des ERM tout en prenant en compte les impératifs poursuivis par l'organisation, à savoir la conformité, l'opérationnel, le stratégique et les informations financières. Les quatre catégories sont mises en relation avec les composantes de la gestion des risques et les processus générés. La figure 3 donne une illustration du cube montrant l'interaction entre les différents éléments.

Certains facteurs vont également augmenter la probabilité de bonne implémentation de l'ERM dans les organisations. Selon une étude, ces facteurs plus présents dans les entreprises auditées par

[6](Source : KPMG. *Placing Value on Entreprise Risk Management* `https://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/documents/Placing-Value-ERM-201003.pdf`)

les Big Four [7], les secteurs de l'éducation, de la banque et de l'assurance ont une probabilité plus élevée d'avoir une bonne implémentation (Beasley et al. 2005).

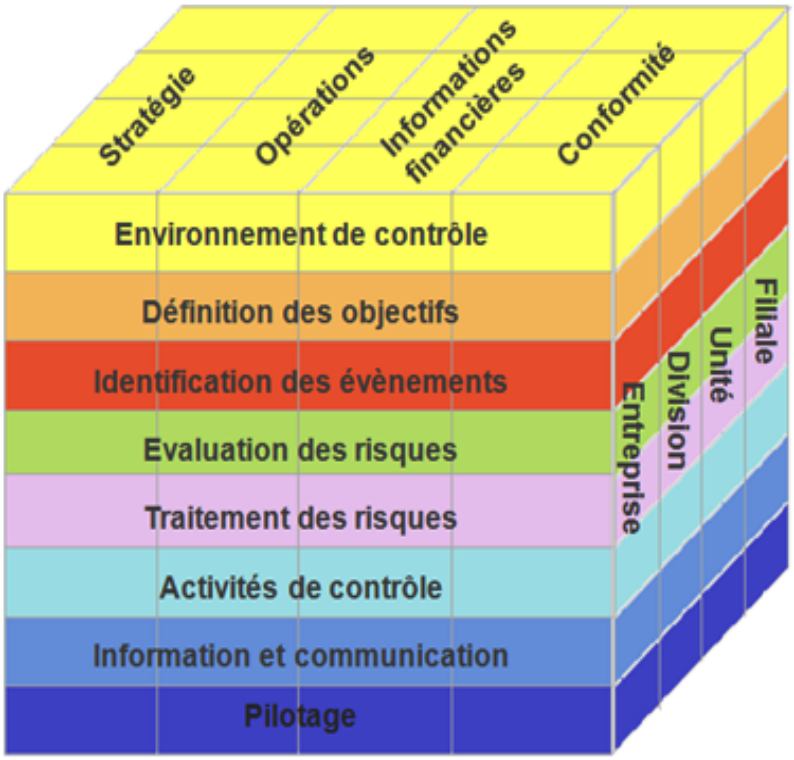


Figure 3: Cube COSO [8]

3.2.1 Environnement interne

L'environnement interne a trait à la culture et à l'esprit de l'organisation. Selon Arena et al. (2010), cette étape permet de déterminer la manière dont le risque est perçu dans l'organisation et d'en définir l'approche par rapport à la gestion du risque. La culture doit être analysée principalement sous deux axes: la culture interne de l'organisation et la culture du risque présente dans l'organisation. Selon Sitkin et Pablo (1992), les membres d'une organisation appréhendent le monde à travers le prisme de la culture de leur organisation, ce qui peut fausser leur perception du risque. Les leaders de l'organisation influencent de manière considérable cette perception du

[7] Comprend les quatres principaux auditeurs au niveau mondiales, à savoir KPMG, Deloitte, PWC et Ernst & Young

[8] (Source : BPMS *L'évolution du référentiel COSO : du contrôle interne au management des risques* `http://www.bpms.info/levolution-du-referentiel-coso-du-controle-interne-au-management-des-risques`

risque dans l'organisation.

Selon Spira et Page (2003), la prise de risques est indispensable pour les activités d'une entreprise. KPMG (2010) définit la culture du risque comme étant un système de valeurs et de comportements présents dans toute l'organisation façonnant la prise de risque. Un jugement critique sur la prise de risque est donc nécessaire de la part de l'ensemble de l'organisation. Sans une culture du risque solide, un ERM, même bien implémenté, peut mener à des mauvaises décisions.

Une étude réalisée par Bozeman et Kingsley (1998) démontre que les managers voulant promouvoir une prise de risque optimale doivent prendre en compte certains éléments. Premièrement, les managers faisant confiance à leurs employés favoriseront une prise de risque calculée au sein de l'organisation. Deuxièmement, la prise de risque est également liée à la définition claire des objectifs de l'organisation. Troisièmement, la bureaucratie et le formalisme sont négativement corrélés avec la prise de risque au sein des organisations. Quatrièmement, un système de récompense favorise la prise de risque au sein des organisations.

L'implémentation d'un ERM dans une organisation est un processus de changement. Certains éléments doivent être pris en compte comme la culture de l'organisation ou le type d'organisation. Un véritable leadership doit se développer pour rendre le processus efficace. Latier (2015) définit le leadership comme permettant de *"développer une vision du futur de l'organisation, la communiquer avec des mots et des actes, motiver et inspirer: produire du changement"*. Certaines autres théories du changement peuvent être envisagées. Nous pouvons notamment citer la théorie développée par Kotter. Ce dernier (1995) a publié un article reprenant huit éléments à prendre en compte pour réussir le processus de changement:

- Etablir un sentiment d'urgence
- Former une coalition de parties prenantes influentes
- Créer une vision
- Donner aux autres le pouvoir d'agir

- Obtenir des résultats à court terme
- Consolider les améliorations et provoquer de nouveaux changements
- Ancrer les changements dans la culture

Selon Latier (2015), il est important d'identifier les agents et destinataires du changement. Les agents sont les instigateurs, concepteurs, exécutants et évaluateurs du changement alors que les destinataires sont les partenaires ou les commanditaires. Il importe de garder à l'esprit qu'une personne peut assumer différents rôles.

Une des méthodes pour analyser la culture présente dans une entreprise nous est donnée par le test OCAI (Oragnizational Culture Assessment Instrument). Ce test individuel permet au travers de questions de déterminer la culture actuelle et souhaitée par les membres de l'organisation (Cameron & Quinn, 2006). Ce test permet à la fois de déterminer si la culture (actuelle ou souhaitée) est tournée vers l'intérieur ou l'extérieur, et si elle est flexible ou stable. Ce dernier, bien que principalement à destination des entreprises du secteur marchand, peut également être utilisé pour déterminer la culture d'une université (Fralinger & Olson, 2007). L'illustration 4 nous donne le tableau d'analyse résultant des tests OCAI. Ce test met en exergue quatre cultures, à savoir la culture de marché, de clan, hiérarchique et adhocratique.

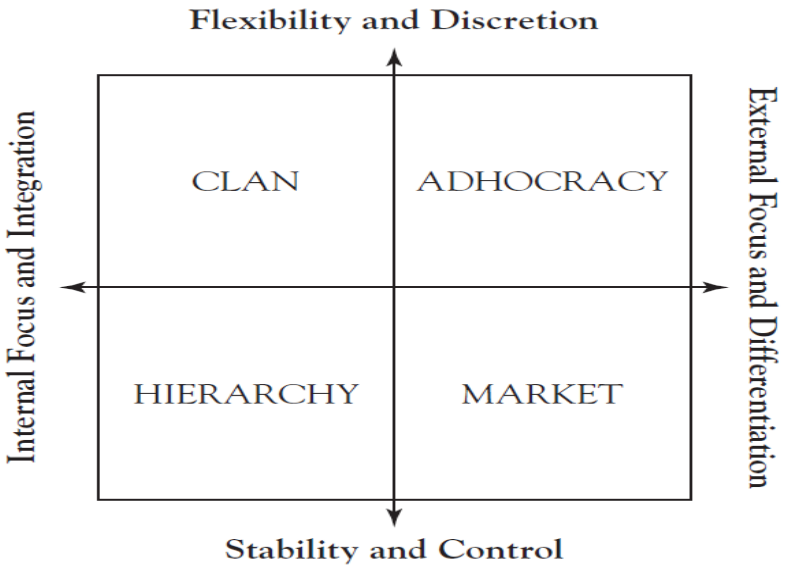


Figure 4: Détermination de la culture à travers un test OCAI [9]

La culture hiérarchique est caractérisée par la structure et la formalisation. Les procédures contrôlent l'action des parties prenantes. Les managers sont appelés à devenir des coordinateurs. Dans ce type d'organisation, les changements sont acceptés de manière relativement rapide.

La culture de marché est caractérisée par la compétitivité et la productivité de l'organisation. Les concurrents sont considérés comme des ennemis, il faut donc prendre toutes les mesures pour lutter contre eux. Dans ce genre d'organisation, les changements sont acceptés s'ils produisent une plus grande compétitivité pour l'organisation.

La culture de clan (ou familiale) est caractérisée par des valeurs et buts partagés, par la participation et l'individualité. Le leader de l'organisation est vu comme un père. Dans ce type d'organisation, les changements ne sont possibles que par la participation et le consensus de l'ensemble de ses membres.

La culture adhocratique est principalement caractérisée par l'adaptabilité, la flexibilité et la

[9]Source: CleverWorkAround *Leave from Article 6 up* `http://www.cleverworkarounds.com/2008/11/`

créativité de l'organisation. Dans ce genre d'organisation, les changements sont considérés comme un challenge et reçus positivement par les différents membres de l'organisation.

3.2.2 Fixation des objectifs

L'objectif de la gestion des risques est de permettre à l'organisation d'atteindre au mieux ses objectifs. Pour pouvoir réaliser une étude de risques, les objectifs doivent être connus préalablement afin de déterminer les éléments pouvant potentiellement influencer leur réalisation. La gestion des risques doit être établie en fonction de la stratégie à long terme de l'organisation mais également sur ses objectifs à court et moyen termes. Les objectifs doivent être coordonnés par rapport à ceux de tous les départements de l'organisation (Kallman et Maric, 2004). La détermination des objectifs sera fonction du type d'organisation, de la structure et du type d'affaire réalisée. Selon la définition de l'ERM du COSO (2004), la manière dont les risques vont être gérés sera dépendante des objectifs.

3.2.3 Identification des évènements

L'identification des évènements doit être réalisée sur bases des objectifs de l'organisation. Selon Williams et al. (1998), l'identification des risques est un processus favorisant la détermination des risques possibles et les conditions augmentant les risques au sein d'une organisation. Kaliprasad (2006) insiste sur le côté proactif de l'identification des évènements. Il s'agit d'analyser tous les risques et opportunités internes à l'entreprise. Certains d'entre eux ne peuvent être analysés que par une coordination entre les différentes fonctions de l'entreprise afin de donner une vue claire et complète de ces risques. Selon Greene et Trieschmann (1984), si l'organisation ne parvient pas à identifier l'ensemble des risques, alors les risques non-identifiés deviendront non-identifiables. L'outil le plus généralement utilisé pour réaliser cette analyse est la cartographie des risques afin d'obtenir une vision claire et globale des risques au sein de l'organisation. La gestion des risques ne peut être réalisée que lorsque les risques ont pu être identifiés. Le challenge est de savoir comment gérer les risques non identifiés. Selon Bookstaber (1999), certains risques ne peuvent pas être gérés directement mais l'identification de caractéristiques augmentera la capacité de réaction et d'identification aux risques.

La réalisation d'une cartographie nécessite plusieurs étapes. L'étape première est l'identification de tous les risques au sein de l'organisation. L'identification permet de mettre en évidence l'exposition d'une organisation à l'incertitude. Pour pouvoir la réaliser, une bonne connaissance des ressources de l'organisation est requise (Tchankova, 2002). L'étude de l'environnement interne et externe dans lequel évolue l'organisation doit également être analysée (Williams et al., 1998). Certaines méthodes peuvent être utilisées pour identifier les risques. Des études et des questionnaires à destination de l'ensemble des membres de l'organisation peuvent donner des éléments indispensables sur l'état des risques. Cependant les résultats de cette méthode peuvent être biaisés. L'utilisation de Flowchart et des états financiers peuvent également aider à l'identification (Head et Horn, 1997). Des inspections peuvent mener à l'identification de problèmes uniques dans l'organisation (Rejda, 1998). Selon Arena et al. (2010), des spécialistes d'une catégorie de risques peuvent également aider à la découverte des risques. Comme Courtot (1998) le souligne dans sa définition (voir supra), la recherche des risques est un processus méthodique. Les risques identifiés peuvent être classés dans plusieurs catégories. Ces catégories peuvent, selon les besoins de l'organisation, être découpées en plusieurs sous-catégories (COSO, 2004).

Une seconde étape de description s'en suit. Les risques sont alors décrits, c'est-à-dire qu'ils sont présentés dans un format structuré donnant ses principales caractéristiques. Par exemple, un tableau reprend tous les éléments pris en considération comme la portée, la nature, les parties prenantes, etc. Cette étape permet de donner aux risques des critères d'évaluation communs à l'ensemble de l'organisation. La gestion du risque étant relativement nouvelle et les risques étant variés, il n'existe actuellement pas de nomenclature internationale sur la dénomination des risques (COSO, 2004).

3.2.4 Evaluation des risques

L'évaluation des risques est l'étape permettant d'attribuer à chaque risque une valeur par rapport aux risques identifiés. Cette étape consiste à recueillir des données sur la probabilité de pertes, sur la gravité et sur la temporalité des risques. (Pritchett, Schmit, Doerpinghauset et Athearn, 1996). Traditionnellement, l'évaluation des risques se base sur la fréquence de l'apparition et de

l'importance du risque (COSO, 2004).

Généralement, les organisations utilisent une échelle fermée pour l'évaluation des risques. Les résultats sont placés dans une matrice graduée de manière identique pour l'évaluation de la fréquence et de l'importance du risque. Plus la graduation de l'échelle sera importante, plus l'analyse sera précise. De plus, les interactions entre les risques et leur environnement doivent également intervenir dans cette partie de l'analyse. C'est également au cours de cette étape que la duplication des risques pourra être mise en évidence.

3.2.5 Traitement des risques

La priorisation des risques doit suivre la phase d'évaluation. Celle-ci permet de mettre en évidence l'importance relative de chaque risque. Selon Maughan (1997), prioriser les différents types de risques selon des critères définis est important pour permettre au gestionnaire des risques d'allouer efficacement les ressources de l'organisation.

Le but de l'évaluation des risques est de prendre une décision en se basant sur les résultats donnés lors de l'étape précédente et des contrôles effectués. L'organisation pourra soit accepter le risque, soit traiter le risque. Le traitement se fera soit par un contrôle, soit par un transfert, soit par une suppression du risque (COSO, 2004). Selon Harrington et Niehaus (1999), une analyse des conséquences quantitatives et qualitatives doit être réalisée pour chaque solution. Kallman et Maric (2004) notent que cette étape consiste à utiliser au mieux les modèles de celle-ci, obtenir le soutien nécessaire et la mise en œuvre du portefeuille des solutions en allouant au mieux les ressources de l'organisation.

Une manière assez simple de voir les différents risques est de créer une carte des risques [10]. Cette carte est une représentation en deux dimensions donnant en abscisse l'impact et en ordonnée la probabilité d'apparition des risques (COSO, 2004). Un exemple de cette cartographie est donné à la figure 5.

[10] appelée en anglais *"heat map"*

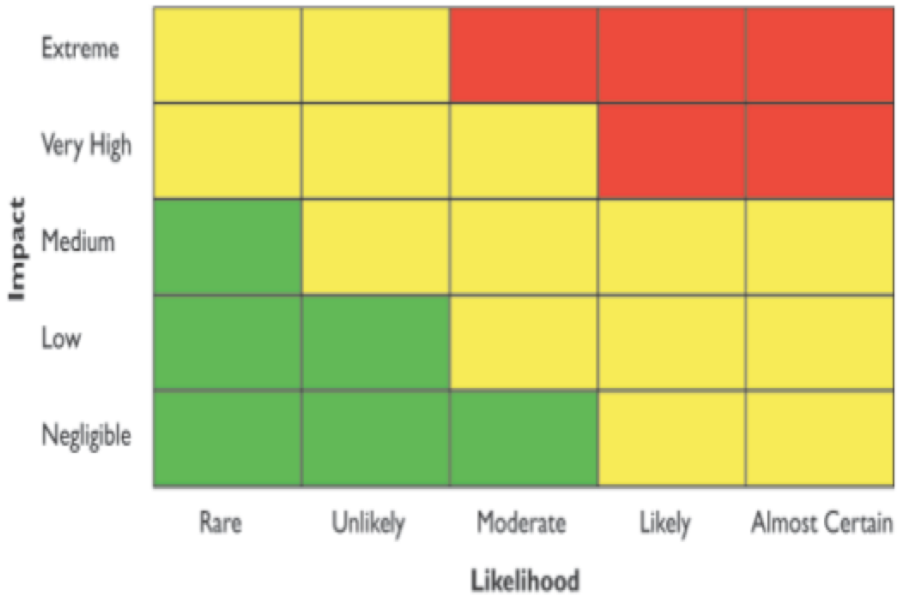


Figure 5: Exemple de cartographie des risques [11]

La gestion des risques peut alors se réaliser de différentes manières et passe généralement par une phase de détermination du plan d'action, reprenant toutes les procédures, plan d'urgence, etc. Par exemple, chez Mega Enterprise Complexity, une entreprise de consulting active notamment dans le secteur de la gestion du risque, la réalisation de cette phase se réalise comme suit: *"Lorsqu'un risque est élevé, le gestionnaire de risques [...] peut décider de l'accepter, de le réduire, de le provisionner, ou de l'assurer. La réduction d'un risque est réalisée par la mise en place de contrôles et de plans d'action. Si les contrôles sont préventifs et pérennes, les plans d'action sont correctifs et bornés dans le temps. La solution permet de soumettre des plans d'action, de les valider par un workflow, et de suivre leur état d'avancement avec des rapports"*.

Cette caractéristique des ERM ne peut être réalisée que par la création de rapports. Ces derniers permettent de conserver une trace de toutes les procédures mises en place.

[11] Source: Visual Manager. *Adding Action and Metaphors to Risk Maps* `http://www.visual-manager.ch/2013/10/09/adding-actions-and-methaphors-to-risk-maps/`

3.2.6 Activités de contrôles

Des procédures et des politiques doivent être décrites en interne afin de veiller à la mise en place effective du processus. Il doit également y avoir un travail de réconciliation entre les procédures externes (par exemple les procédures de conformité) et les procédures internes (par exemple les cas de fraude).

La création de rapports est un élément permettant de faciliter les différentes activités de contrôle. Elle permettra de vérifier la bonne implémentation des plans d'action déterminés et de mesurer leur efficacité (CS Star, 2006).

3.2.7 Informations et communications

La gestion du risque est l'affaire de tous. Le rôle du management est de promouvoir, au sein de l'organisation, la publicité des procédures de manière verticale et transversale de la façon la plus efficace possible (COSO, 2004). La documentation doit résumer les objectifs de l'organisation, les risques, les solutions et la méthodologie décisionnelle. Le but des rapports est de fournir aux parties prenantes un résumé des activités de création de valeur du gestionnaire de risque. Ce document sert aussi comme point de départ pour la prochaine itération du processus de gestion des risques (Pritchett et al. , 1996). Selon Kallman et Maric (2004), une fois qu'une décision a été prise, les solutions doivent être conservées et mises sur un support à destination des parties prenantes. Dans le cas où aucun support n'est alloué les solutions de gestion des risques sont susceptibles d'échouer et de ne pas atteindre le succès escompté (Baily & Petersen, 1989). Il faut veiller à ce que ces informations soient facilement accessibles pour l'ensemble des parties prenantes à la gestion des risques. Elles peuvent, par exemple, être mises dans un "Sharepoint" ou autre module de communication interne de l'organisation.

Un langage commun doit également être communiqué à l'ensemble de l'organisation. Selon Acharyya (2009), un ERM peut fournir un langage commun pour la description des risques et des conséquences, pouvant mener à une amélioration de la communication dans l'entreprise. Cette étape comprend également la phase de reporting vers les instances de l'organisation. Selon

McKinsey & Company (2010), il est précisé que le rapport sur les risques à destination du management ne peut être utilisable que s'il est perspicace et bien synchronisé. Le rapport doit mettre en évidence les risques les plus importants et le traitement proposé à ceux-ci. Un rapport trop détaillé peut rendre l'information inutilisable pour le management. Le gestionnaire du risque doit avoir des capacités dans le tri de l'information. Selon l'HCCA Audit & Compliance Committe Academy (2011), les rapports sur la gestion des risques doivent contenir certaines informations telles que les connections entre les différents exercices, les mises en évidence des anciens et des nouveaux risques et les vérifications qui ont été effectuées.

Il est souvent important de protéger ce genre de données. Ces dernières peuvent s'avérer sensibles si elles venaient à être diffusées.

3.2.8 Pilotage

La gestion des risques est un processus itératif et dynamique (Courtot, 1998 ; Kallman et Maric, 2004). Head and Horn (1997) insiste sur l'importance de cette étape pour obtenir des résultats du programme sur le long terme. Cette étape demande à l'organisation de mettre sur pied des processus de contrôle des activités et de vérifier l'efficacité de chaque étape du système de gestion des risques dans l'organisation. Elle permet d'effectuer les modifications nécessaires au besoin de l'ERM. Ces modifications peuvent se réaliser par des activités de gestion continues, des évaluations séparées de chaque élément ou une combinaison des deux méthodes. (COSO, 2004). Selon Nelson et Ambrosini (2007), le pilotage est l'étape permettant à l'ensemble du processus de tenir et que sans cette étape, l'ERM deviendrait inefficace. Selon Power (2009), le pilotage de l'ERM doit se faire sur l'ensemble de l'organisation et des processus. Les ajustements doivent être réalisés en fonction des erreurs du passé et des changements d'environnement (aussi bien internes qu'externes).

3.3 Rôles et responsabilités

Selon le COSO, *"Le management des risques est l'affaire de tous mais, in fine, le directeur général en est le propriétaire et en assume la responsabilité. Les autres managers soutiennent la culture en matière de management des risques, ils œuvrent pour sa mise en conformité avec*

l'appétence pour le risque. Ils gèrent aussi les risques au sein de leur périmètre de responsabilité dans les limites de la tolérance au risque [...] Le conseil d'administration exerce une activité de surveillance sur le dispositif de management des risques, il a connaissance et valide l'appétence pour le risque de l'organisation"(COSO, 2004, p. 14). Cette définition met en avant le rôle central du Management dans l'implémentation de l'ERM. En effet, l'impulsion doit venir de la personne assumant la responsabilité finale, c'est-à-dire le directeur de l'organisation. De plus, le bon fonctionnement du programme sera positivement corrélé avec l'attitude du management dans l'implémentation (Bozeman et Kingsley 1998).

De facto, la gestion effective des risques est déléguée à d'autres départements de l'organisation spécialisée dans le risque. Le gestionnaire du risque et l'auditeur interne assument, dans de nombreux cas, conjointement, les responsabilités fondamentales de la gestion des risques. Selon Sarens et Christopher (2015), la gestion des risques peut être réalisée soit par le département d'audit interne, soit par un département de gestion du risque ou soit par une externalisation de la gestion des risques.

L'*Institute of Risk Management* (IRM) définit le rôle du gestionnaire du risque comme celui qui a la qualification nécessaire pour être responsable de l'identification des risques au sein de l'organisation et du traitement de ceux-ci. Le gestionnaire du risque ne doit pas compter uniquement sur ses savoirs. Jorion (2008) insiste sur le fait *"qu'une gestion du risque formelle ne peut pas se substituer à l'expérience"* (p.53).

L'*Institut Français de l'Audit et du Contrôle Interne* (IFACI, 2000) définit l'audit interne comme étant *"une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée. Il aide cette organisation 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, et en faisant des propositions pour renforcer leur efficacité"*. L'*Institute of Internal Auditors* (IIA) donnera à l'Auditeur Interne la responsabilité d'apporter aux parties prenantes une certaine assurance sur la conformité des politiques mises en place pour

atténuer les risques et sur l'efficacité de la politique de gestion du risque (IIA, 2004).

L'illustration 6 tirée du site de l'IIA, donne les rôles devant être accomplis par l'auditeur interne (en bleu foncé), ceux pouvant être accomplis à la fois par l'auditeur ou par une autre personne (comme le gestionnaire du risque) (en bleu clair) et les fonctions ne pouvant dans aucun cas être réalisées par l'auditeur interne mais devant être accomplies par une autre personne de l'organisation (comme le gestionnaire du risque) (en gris).

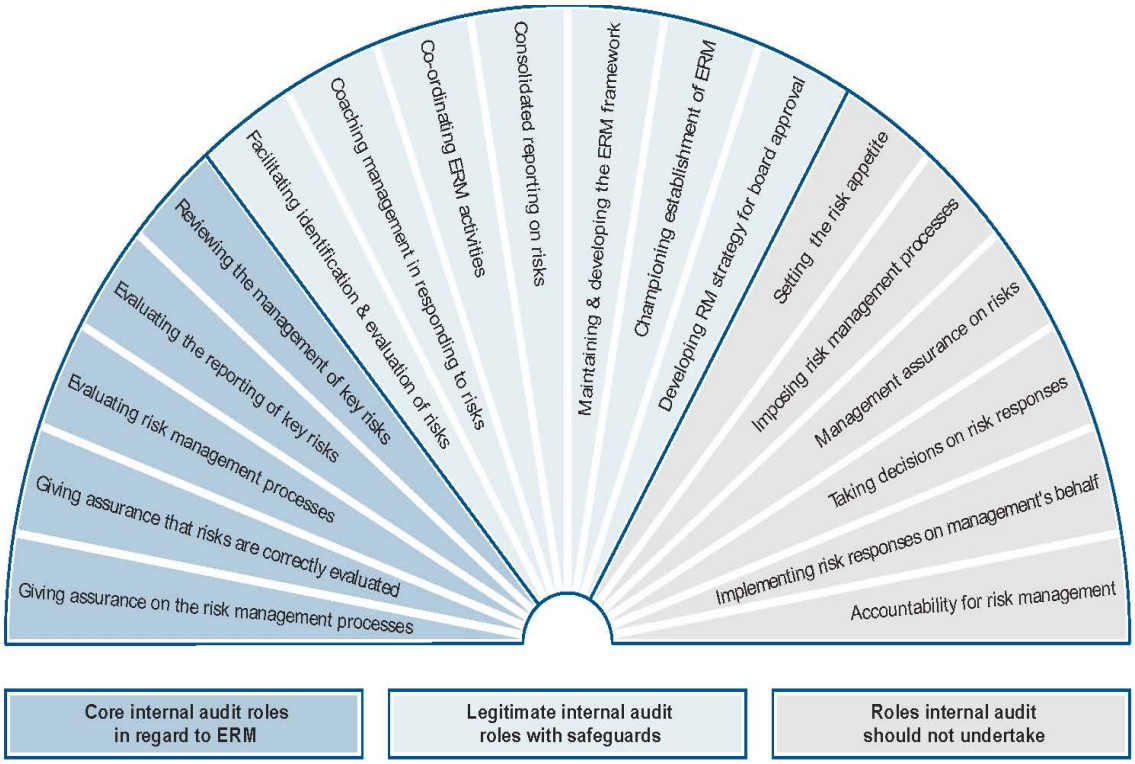


Figure 6: Rôle de l'audit Interne dans la gestion du risque [12]

Les auditeurs internes étaient vus dans le passé comme des *"policemen and watchdog"* (Douglas, 1999) de l'entreprise, subordonnés aux fonctions majeures de l'organisation et considérés comme un facteur coût à minimiser. Ils étaient vus comme étant des spécialistes du contrôle interne sans être considérés comme importants pour la stratégie de l'entreprise (Spira et

[12]Source: IIA, *The Role of Internal Auditor in Risk Management*. https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Role%20of%20Internal%20Auditing%20in%20Enterprise%20Risk%20Management.pdf

Page, 2003). Suite aux nombreux scandales financiers et crises, dus notamment au manque de contrôle adéquat (Jorion, 2008), ces fonctions sont devenues centrales aujourd'hui et apportent une valeur ajoutée considérable à l'entreprise. Leur statut est passé de celui de contrôleur à celui de *"contrôleur-conseiller"* du management (Morgan, 1979). L'idée de gestion du risque est fortement liée avec celle de contrôle interne par la considération que le risque peut être objectivé, identifié et quantifié, ce qui le rend gérable pour l'organisation. Selon Spira et Page (2003), cette redéfinition de contrôle interne comme gestion du risque renforce le rôle de ces contrôles comme étant une fonction stratégique et de support pour l'organisation.

Les auditeurs internes et les gestionnaires du risque sont avant tout présents pour protéger les actionnaires dans une optique d'audit *"stakeholder-oriented apporach"* (Niamh & Solomon, 2008). On retrouve cette idée dans différents codes de bonne gouvernance tels que The Cadbury Report (1992) ou The Higgs Report (2003). Les nouvelles définitions des différents rapports publiés sur le sujet tendent à donner à l'audit interne un rôle plus proactif dans ce management du risque.

Une grande distinction entre la fonction d'auditeur et de gestionnaire du risque réside dans l'indépendance. En effet, l'auditeur réalisera son travail en toute indépendance vis-à-vis du management, ce qui ne sera pas le cas du gestionnaire du risque. Les deux fonctions principales de la gestion des risques partagent par ailleurs *"en commun certains savoirs, certaines qualifications et certaines valeurs"* (IIA, 2004). Par contre, in fine, les auditeurs internes et les gestionnaires du risque ne rapportent pas aux mêmes instances des organisations. Les auditeurs internes rapportent directement au comité d'audit tandis que les rapports des gestionnaires du risque sont adressés à la direction de l'organisation. L'IIA insiste sur le fait que l'auditeur ne doit pas sous-estimer les savoirs spécifiques requis pour la fonction de gestionnaire du risque (IIA, 2004).

Selon une étude réalisée par Beasley et al. (2005), la présence d'un *"champion du risque"* augmente de manière significative la bonne implémentation d'un ERM dans une organisation. Le champion du risque est défini par l'IIA comme étant :*"la personne devant promouvoir la gestion du risque et ses avantages à travers l'organisation. Il doit pour accomplir son rôle éduquer les*

parties prenantes et insuffler la volonté au sein de l'ensemble de l'organisation" (IIA, 2009). L'auditeur peut prendre le leadership de la gestion des risques et être le *"champion du risque"*. En effet, selon l'IIA, l'auditeur interne, par sa compréhension des mécanismes internes, est qualifié pour agir en tant que gestionnaire de projet de l'ERM, en particulier pour l'établissement des premières phases de l'implémentation (IIA, 2009). Dans le cas où les fonctions d'auditeur et de champion du risque sont séparées, les deux fonctions devront être perçues comme complémentaires et les rôles respectifs doivent être clairement définis par l'organisation afin de garantir l'efficacité du processus. Celui-ci permet également d'éviter une concurrence inutile entre les fonctions. Cette concurrence pourrait mener à une duplication inutile de la gestion. (IIA, 2009)

Selon Arena et al. (2010), il existe également une autre fonction en rapport avec la gestion des risques: le spécialiste d'une catégorie de risques. Les auditeurs et les *"Champion du risque"* ne peuvent se substituer à lui. Le gestionnaire du risque (qu'il soit auditeur ou non) ne doit pas être un expert de tous les risques mais doit servir de conseiller au management dans sa prise de responsabilité par rapport aux risques existants. En d'autres termes, demander à l'auditeur ou au gestionnaire du risque de remplacer l'expert peut avoir l'effet inverse de celui escompté. Selon Spira et Page (2003), de nombreuses organisations ont ajouté dans leur département de gestion du risque des spécialistes (par exemple des ingénieurs ou des marketeurs) pour améliorer le fonctionnement de ceux-ci. Selon Power (2007), des spécialistes, possédant les qualifications et compétences pour gérer une catégories de risques, doivent être identifiés au sein de l'organisation.

Les principes de la gestion du risque étant relativement nouveaux, de nombreux auditeurs internes et gestionnaires du risque sont dans une zone d'incertitude sur certains points comme la terminologie, la métrologie et le rôle qu'ils doivent jouer dans ce nouveau concept. (Coetzee & Lubbe, 2014)

Les acteurs de la gestion des risques ont de nombreux outils à leur disposition pour mettre en place un programme de gestion du risque. Les principaux sont ceux du COSO (COSO's ERM), de l'ISO (ISO Risk Management), du Rank Group (Turnbull Code) et celui de la FERMA (A Risk Management Standard by the Federation of European Risk Management Associations).

3.4 Valeurs ajoutées de la gestion des risques

Cette gestion du risque a favorisé l'émergence d'une nouvelle fonction dans l'entreprise, celle de gestionnaire du risque au sein des entreprises mais donne également de nouvelles responsabilités à l'auditeur interne. En audit interne, ce changement se traduit par une redéfinition de la manière d'auditer. Les rapports d'audit sont principalement basés sur le risque (Coetzee & Lubbe, 2014).

Une enquête réalisée par Proviti, TNS, Sofres & l'Expansion auprès de 100 directeurs financiers en 2003 a mis en évidence que la gestion des risques apporte une valeur ajoutée considérable aux entreprises. En effet, en plus de réduire l'impact des risques, elle fournit aux organisations une masse d'informations déterminantes pour la bonne marche de l'organisation et le pilotage de sa performance (Aubry, 2012). Une étude réalisée par PWC entre 2008 et 2012 sur le métier d'auditeur montre qu'un des changements fondamentaux dans la profession est l'incorporation de la gestion du risque et que cette dernière apporte une valeur ajoutée considérable à l'entreprise. (PWC, 2012)

Cette nouvelle définition élargit le domaine d'activité de la fonction d'auditeur, reconnaissant son rôle majeur tant dans la gouvernance de l'entreprise que dans la gestion des risques. On montre la valeur ajoutée d'une fonction longtemps considérée comme étant uniquement un facteur de coûts pour l'entreprise. L'auditeur interne doit désormais connaître la stratégie de l'entreprise et être associé à cette dernière (IIA, 2012).

Selon McKinsey & Company (2008), la gestion du risque est une discipline offensive qui peut, si elle est correctement implémentée, maximiser la valeur de l'entreprise. Cette discipline est seulement en train d'émerger et de nombreuses entreprises ne l'utilisent pas de manière adéquate pour augmenter la valeur que cette dernière peut représenter. Comme le paraphrase McNamee et McNamee (1995), les auditeurs internes rompent avec leurs racines comptables pour apporter une valeur ajoutée au management.

4 Gestion des risques dans les universités

La gestion du risque est devenue ces dernières années d'une importance capitale pour les organisations (Arena et al., 2010). Ce processus, ayant été implémenté dans de nombreuses organisations à travers le monde, se veut être une aide pour l'atteinte de leurs objectifs.

La gestion du risque, mise en œuvre en réponse aux problèmes de gestion des entreprises du secteur privé (Baker, 2009), s'est vite élargie à d'autres types d'organisation dont les universités. Les entreprises du secteur privé et les universités ne partagent pas les mêmes objectifs. Néanmoins, les deux types d'organisations affrontent de nombreux risques qui doivent être gérés de manière identique. De nombreux éléments de la gestion restent semblables et les codes de références en la matière de risques sont les mêmes (COSO, 2004, ISO, 2009).

Actuellement, de nombreuses universités à travers le monde ont mis sur pied une politique de gestion du risque. Ces universités appartiennent principalement au monde anglo-saxon. Nous pouvons citer comme exemples l'Université de Cambridge (USA), l'Université de Stanford (USA), L'Université Heriot-Watt (UK- Ecosse) ou l'Université de Pretoria (Afrique du Sud). Ces universités peuvent être publiques comme l'Université de Cambridge ou privées comme l'Université de Stanford.

Les différentes universités mettent en avant les avantages de l'utilisation d'un tel outil. L'Université de Pretoria affirme à propos de la gestion des risques que *"Nous voulons ajouter de la valeur et améliorer la prise de décision à l'université dans la recherche de l'excellence à travers la gestion du risque et les activités d'audit interne"* (University of Pretoria, 2015).

Pour comprendre la gestion d'une organisation, il faut connaître l'ensemble des activités qu'elle serait amenée à réaliser mais également s'intéresser à l'essence de ce type d'organisation. La notion d'université a fortement évolué au cours du temps. Au Moyen Age, celle-ci était *"une institution ecclésiastique jouissant de privilèges royaux et pontificaux et chargée de l'enseignement"* (Larousse, 2008). Denman (2005) donne une définition moderne de ce qu'est une université.

C'est un *"établissement d'enseignement supérieur complexe, formellement autorisé à proposer et à délivrer des diplômes de haut niveau dans au moins trois disciplines ou domaines d'études"* (Denman, 2005, p.19). Il s'agit donc d'une organisation où le but principal est la transmission du savoir.

A l'heure actuelle, les universités sont de plus en plus soumises à un processus de mondialisation (Scott, 1998). Selon l'OCDE, les motifs de cette mondialisation sont à la fois politiques, économiques, universitaires et sociaux. Cette internationalisation a également comme conséquence d'augmenter la compétitivité entre les différentes universités. Cette évolution rend les universités de plus en plus compétitives et les incite à utiliser les nouvelles méthodes de management dans le but d'obtenir le plus grand nombre possible de facteurs clés de succès (Kehm et Lanzendorf, 2006).

Traditionnellement, l'université poursuit plusieurs missions qui peuvent varier selon le contexte. Les objectifs peuvent évoluer en fonction du pays, du type d'enseignement et du secteur (public ou privé) dans lequel l'université se déploie (Morphew et Hartley, 2006). En Fédération Wallonie-Bruxelles, l'article 3 du décret du 31 mars 2004 définit que les missions des établissements supérieurs sont l'enseignement, la recherche et les services à la société.

De plus, les universités possèdent ou gèrent généralement des spin-off, des ASBL et autres organisations leur permettant de mener à bien leurs missions. Pour pouvoir réaliser celles-ci, les universités doivent attirer des étudiants, des chercheurs mais également des sources de financements extra-muros.

Tous ces éléments sont facteurs de risques, et une mauvaise gestion de ceux-ci pourrait empêcher la réalisation des objectifs des universités. Par exemple, un problème d'image pourra avoir comme conséquence une diminution du nombre d'étudiants ou la fin d'une collaboration avec une entreprise entraînant par la même occasion une diminution des ressources nécessaires aux missions. Nous pouvons noter que dans de nombreux pays anglo-saxons, les régulateurs et/ou législateurs fournissent des guides de bonne gouvernance (Higher Education Act (UK), Association of Governing Boards (USA), Education Amendment Act (Afrique du Sud)). Ces

guides, qui sont dédiés totalement ou en partie aux universités, conseillent aux institutions d'implémenter un processus de gestion des risques. La mise en œuvre d'un tel projet est dans de nombreux cas, comme par exemple pour le Higher Education Act, accompagnée de subventions.

Une étude réalisée par Christopher et Sarens (2015) sur la gestion du risque dans les universités publiques australiennes montre que l'influence clé de la mise en œuvre est la législation en vigueur se voulant *Business Like* (Higher Education Act, 2003). La mise en place d'un programme de gestion des risques dans une université doit prendre en compte les visions des différentes parties prenantes, aussi bien au niveau stratégique qu'opérationnel. Selon cette étude, la gestion effective dans les universités australiennes est réalisée, soit par le département d'audit interne, soit par un département exclusivement dédié à la gestion des risques, ou soit par un département extérieur à l'université.

De nombreuses universités ayant implémenté un processus de gestion des risques en leur sein publient sur leur site internet des informations relatives à leur ERM (Université de Cambridge, Université d'Aberdeen, Université de Denver, Institut de Technologie de Californie). Nous pouvons noter que ces universités sont soumises à une législation plus stricte en matière de gestion des risques (Highter Education Act, Higher Education Opportunity Act). La législation va soit obliger l'université à implémenter le programme comme c'est le cas pour l'Université de Denver par le Higher Education Opportunity Act ou accorder des subventions supplémentaires comme prévu par le Higher Education Act pour les universités anglaises du secteur public. Les documents en accès libre donnent principalement une série d'indications sur la législation, l'identification, la réponse aux risques et la coordination entre les différentes parties prenantes. Peu d'informations sont disponibles sur la culture de l'organisation mise à part l'influence que les risques peuvent avoir sur les objectifs généraux des universités. Pour l'identification des risques, celle-ci donne une série de pistes de réflexions.

> **Exemple:** l'Université de Cambridge réalise des séances de brainstorming, étudie les expériences du passé, les facteurs internes et externes et établit des hypothèses.

Une fois les risques identifiés, les universités analysent de la manière la plus constructive

possible la réponse la plus optimale à apporter aux risques. D'un point de vue opérationnel, la gestion des risques englobe l'entièreté des contrôles et fonctions de l'université. Nous pouvons également noter que ce n'est pas forcément le département d'audit qui prendra le leadership dans la gestion des risques mais sera néanmoins intégré au processus comme pour la surveillance des opérations.

Exemple: l'Université de Denver montre de manière schématique à la figure 7 l'intégration des différents départements de l'université dans la gestion des risques. On peut noter que dans le cas de Denver, le comité d'audit ne gère pas le risque mais vérifie la conformité du programme.

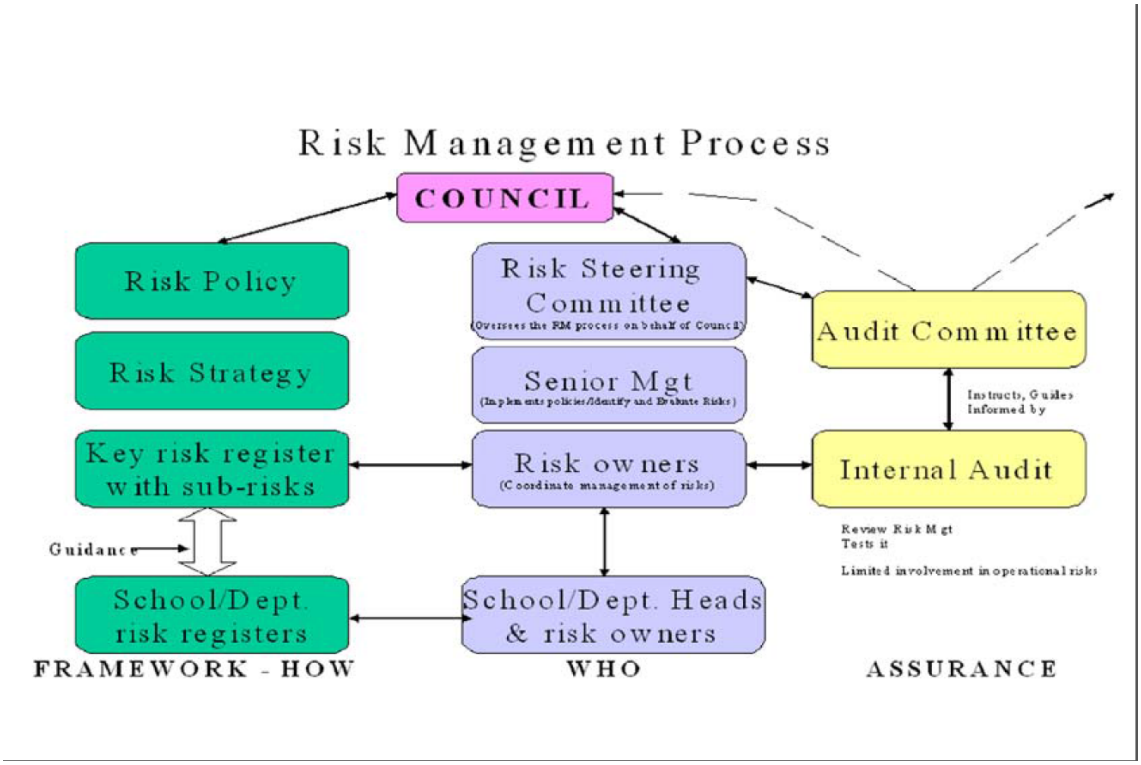


Figure 7: Processus de gestion du risque à l'Université de Denver [13]

Actuellement, la Fédération Wallonie-Bruxelles n'impose et ne favorise pas la mise en place d'un système de gestion du risque dans ses universités. Les universités dépendantes d'elle sont

[13] Source: University of Denver *Policy of Risk Management* `http://www.du.edu/risk/policy.html`

soumises à une forte concurrence sur le marché tant national qu'international, doivent se démarquer les unes des autres et trouver des financements supplémentaires (Leclercq, 1999). La gestion des risques offre un outil de bonne gestion qui pourrait, dans le cas d'une bonne implémentation, apporter une valeur ajoutée à l'université. Ce mémoire tentera de voir comment et dans quelle mesure un tel processus peut être éventuellement mis sur pied.

Partie II: Conditions d'implémentation d'un processus de gestion du risque à l'Université catholique de Louvain

1 Propédeutique du mémoire

L'Université catholique de Louvain ne possède actuellement aucun processus structuré de gestion des risques. Les risques sont gérés de manière indépendante par silos organisationnels et en bon père de famille. Suite à une constatation provenant du département des risques et patrimoine financier, une réflexion a émergé. Ce département, gérant les polices d'assurance de l'université, a mis en évidence un problème dans les contrats, provenant d'une mauvaise estimation des différents risques de l'Université.

Une étude exploratoire a été réalisée en 2011 sur la gestion des risques. Les résultats de cette études sont donnés ci-après au point 3. Ce mémoire se veut être une continuation de cette étude exploratoire. C'est pourquoi une série d'interviews de différents directeurs du CODIR ont été réalisées. Le résumé de ces interviews se trouve au point 4.

Sur base de ces résultats et de l'étude exploratoire réalisée, nous tenterons ultérieurement de déterminer dans quelle mesure il est possible d'implémenter un processus de gestion du risque à l'UCL.

2 Présentation de l'Université catholique de Louvain

L'institution dans laquelle nous avons réalisé l'étude de cas est l'Université catholique de Louvain. Il s'agit d'une université belge située en Fédération Wallonie-Bruxelles . C'est une université de premier plan ouverte sur le monde. En effet plus de 127 nationalités s'y côtoient et elle fait partie de plusieurs associations internationales universitaires comme le Groupe de

Coimbra ou l'IMCC. Riche de 600 ans d'histoire, elle figure parmi les plus vieilles universités d'Europe (UCL, 2011).

Le statut juridique de l'Université catholique de Louvain est celui d'*"une personne morale de droit privé poursuivant un but d'utilité publique et jouissant de la personnalité civile"* [14] (UCL, 2011). Son siège administratif est situé en Belgique à Ottignies-Louvain-la-Neuve.

L'institution poursuit une triple mission, à savoir l'enseignement, la recherche et les services à la société. Ces objectifs sont inscrits dans les statuts de l'université.

Elle est répartie sur 6 sites dispersés sur le territoire de la Fédération Wallonie-Bruxelles (principalement localisés à Ottignies-Louvain-la-Neuve mais également à Mons, Charleroi, Tournai et Bruxelles (sites de Saint Gilles et Woluwe-Saint-Pierre)). Ses activités d'enseignement sont dispensées par 14 facultés et la recherche est effectuée à travers les 21 instituts. Elle participe également à certaines ASBL (dont les hôpitaux universitaires, les bibliothèques, les parcs scientifiques et le musée universitaire). Elle gère aussi un staff de 5 691 enseignants, chercheurs, collaborateurs administratifs et techniques (chiffres 2013) et 28 840 étudiants (chiffres 2013). Elle est en outre propriétaire d'un parc immobilier de plus de 3500 logements (chiffres 2011-2012) et de nombreuses infrastructures sportives.

L'administration est composée de 23 départements s'occupant de manière transversale de toute la partie administrative de l'université. Il s'agit de départements s'occupant d'éléments variés, comme les infrastructures informatiques, les services aux étudiants ou les finances de l'université.

L'université est dirigée par un pouvoir organisateur composé des évêques francophones de Belgique et d'un conseil d'administration composé de membres internes et externes de l'institution.

[14] Loi du 12 août 1911 accordant la personnalité civile à l'"Université Catholique de Louvain – Katholieke Universiteit te Leuven", à l'"Université libre de Bruxelles" et à la " Vrije Universiteit Brussel", et autorisant l'"Université Catholique de Louvain – Katholieke Universiteit te Leuven" à créer une université de langue française et une université de langue néerlandaise, *M.B.* 1911 modifiée par la loi du 28 mai 1970, *M.B.* 1970 et par le Décr. Com. fr. du 31 mars 2014, *M.B.* 2014

La direction est assurée par un recteur, élu par ses pairs, collaborateurs et étudiants. Ce dernier délègue une partie de ses prérogatives à des vice-recteurs et la gestion de la partie administrative à un administrateur général. Le graphique 8 représente de manière schématique l'organisation de l'UCL.

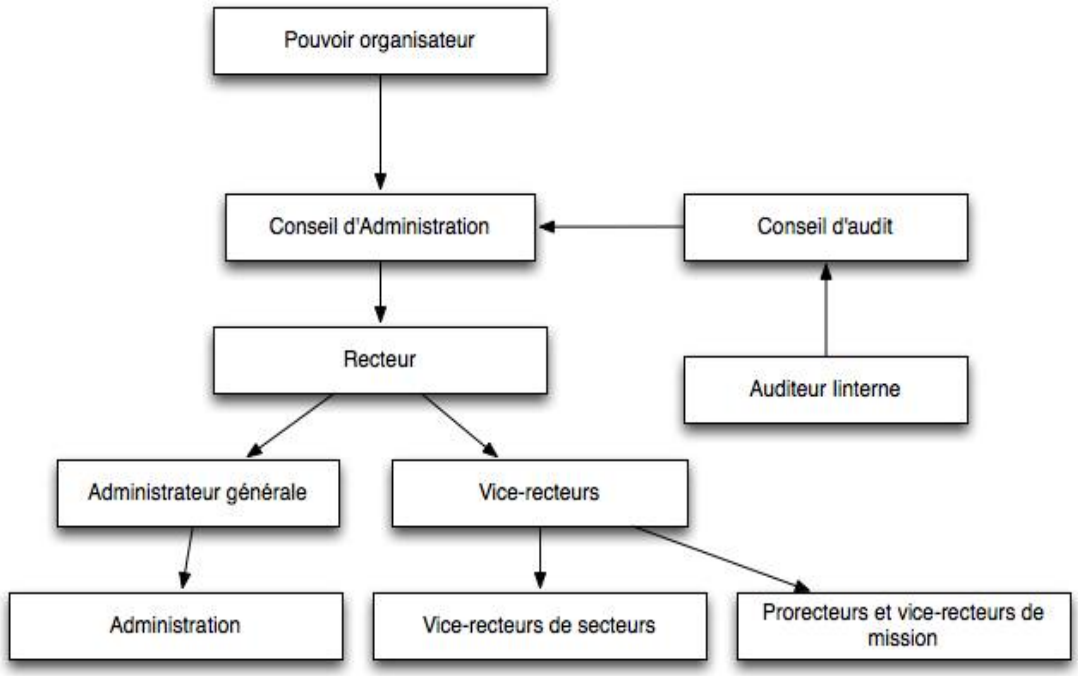


Figure 8: Organisation de l'UCL

Les 14 facultés et les 21 instituts possèdent une administration interne qui leur est propre. Les facultés sont gérées par un doyen et les instituts par un directeur.

Pour pouvoir assumer au mieux toutes ses missions, elle doit trouver des financements extérieurs. L'université, bien que privée, est financée en grande partie par la Fédération Wallonie-Bruxelles qui *"contribue, par des allocations annuelles, au financement des dépenses de fonctionnement"*[15]. Ces allocations comprennent une partie fixe, revue tous les 10 ans et une partie variable liée au nombre d'étudiants inscrits chaque année. Elles englobent les dépenses

[15]Loi du 27 juillet 1971 relative au financement et le contrôle des institutions universitaires, art. 25, *M.B.* 1971

administratives, d'enseignement et de recherche. Les autorités fédérales et régionales financent également de nombreux projets de recherches.

L'université recourt également à d'autres sources de financement. On peut notamment citer les financements privés. L'université s'est dotée d'une fondation (Fondation Louvain) permettant à des mécènes d'aider divers projets de l'UCL comme la recherche, les musées, des bourses d'études, etc. L'institution reçoit également des financements étrangers, principalement de l'Union Européenne dans le but de favoriser la coopération entre universités européennes ou encore le projet PCRD 7.

Enfin, les instituts de recherche doivent trouver dans de nombreux cas des financements extérieurs pour réaliser leurs projets, l'institution ne couvrant que leurs frais de fonctionnement minimaux.

L'université possède une certaine visibilité sur le plan international, conclut des accords avec de nombreuses universités à travers le monde et participe notamment aux programmes Erasmus et Mercator.

3 Etude exploratoire

Une étude exploratoire a été réalisée à l'initiative du directeur du département des risques et patrimoines avec l'accord de l'administrateur général. Ce mémoire se propose d'être une continuation de ce travail, initié en 2008. L'étude est partie d'une réflexion sur la gestion des risques à l'Université catholique de Louvain. Elle part *"du postulat que l'externalisation (prise d'assurance) correcte des risques ne peut se réaliser que par la bonne connaissance des risques présents."* (Rombouts, 2013)

Les premiers résultats ont été présentés à l'administrateur général de l'UCL en janvier 2013. Ce document, intitulé *"Gestion des risques - Etude exploratoire: risques perçus par les membres*

du CODIR", s'appuie sur quelques principes théoriques et sur des interviews auprès d'un groupe cible, à savoir les membres du CODIR.

Ce rapport doit être considéré, comme indiqué dans l'introduction, comme un document de travail, ne contenant ni recommandation, ni suggestion sur la manière d'implémenter les risques à l'UCL.

Ce travail a comme fondement théorique des sources qui ont également servi de base à la réalisation de ce mémoire, à savoir les rapports publiés par le COSO, l'ISO et la FERMA.

Le document se compose d'une partie théorique, reprenant la définition et la classification des risques, les bases théoriques de la cartographie de ceux-ci, la mise en œuvre d'un système de gestion des risques ainsi que les rôles et responsabilités de cette gestion. Il donne également une série d'exemples concrets d'implémentation dans diverses universités américaines, à savoir l'Université de Columbia, l'Université de Californie, l'Université de Stanford et l'Université Texas A&M.

Les résultats de cette étude donnent une première cartographie des risques. La méthode utilisée pour leur détermination est l'identification spontanée des risques par les membres du CODIR. Ces derniers devaient répondre à un questionnaire reprenant leur définition du risque ainsi qu'une classification sur une échelle de 1 à 5 des risques rencontrés par leur entité. La cartographie a été réalisée département par département sans coordination des différentes cartographies.

La recherche exploratoire a permis de démontrer que 271 risques étaient mis en évidence par les différentes entités du CODIR. Les risques de niveau 1 (très importants) étaient au nombre de 31.

La nature des risques exprimés a pu être décomposée en grandes catégories, à savoir :

- Risque stratégique et politique
- Risque structurel offre/demande enseignement/recherche

- Risque *"étudiant"*
- Risque opérationnel

Une nomenclature indicative a également été proposée pour permettre l'éclatement des différents risques cités. Cette nomenclature ne peut être définitive sans la nomination de coordinateurs locaux des risques. La figure 9 reprend l'ensemble des risques rencontrés par chaque département du CODIR ainsi que leurs risques de niveau 1 (niveau le plus important de la classification).

Entité	Priorité 1	Nombre de risques cités	Entité	Priorité 1	Nombre de risques cités	Entité	Priorité 1	Nombre de risques cités
ADAE	2	12	AREC	1	10	INESU	1	9
ADEF	2	5	AUD	0	2	RHUM	4	12
ADFI	0	15	BIUL	1	12	SERP	2	12
ADMG&CADG	1	17	CRCT	2	6	SET	0	6
ADPI	1	17	SSH	0	10	SGSI	1	8
ADRE	5	31	SST	1	10	SPER	1	8
ADRI	0	5	SSS	4	12	UCL MONS	2	9

Figure 9: Risques par entité à l'UCL [16]

L'illustration 10 reprend de manière agrégée les risques donnés par les différents membres du CODIR, le pourcentage relatif de chaque catégorie de risque et entre parenthèses le nombre de fois que le risque est cité.

Un projet de gestion des risques a également été proposé par l'étude exploratoire. L'illustration 11 montre la dynamique du traitement des risques. D'un côté, les entités génératrices de risques et de l'autre les coordinateurs locaux de risques. Au centre, le coordinateur sert de hub entre les coordinateurs locaux, les générateurs et le management.

[16]Source: *Gestion des risques - Etude exploratoire: risques perçus par les membres du CODIR*

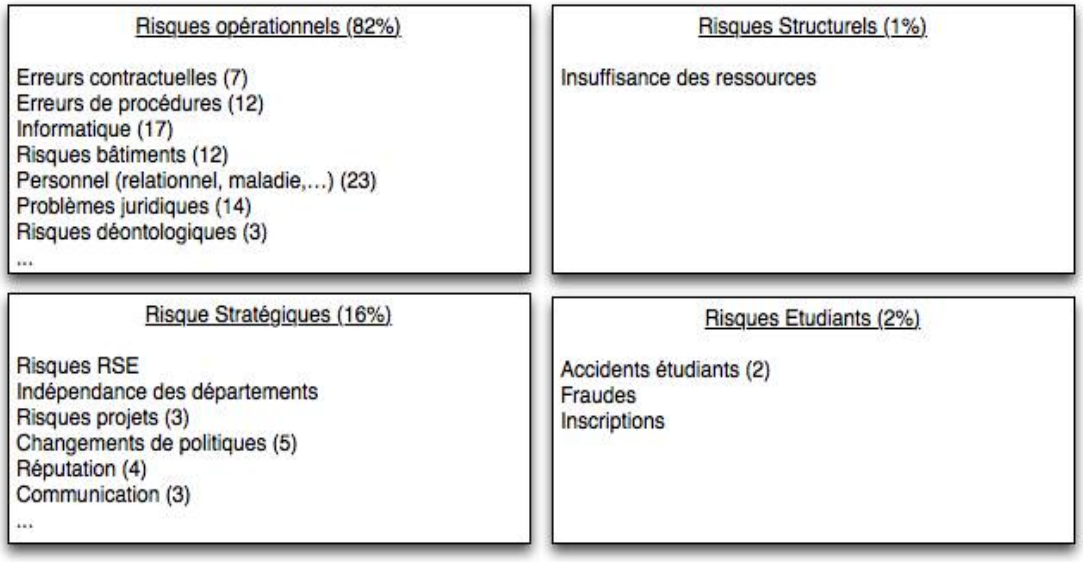


Figure 10: Risques agrégés donnés lors de l'étude exploratoire

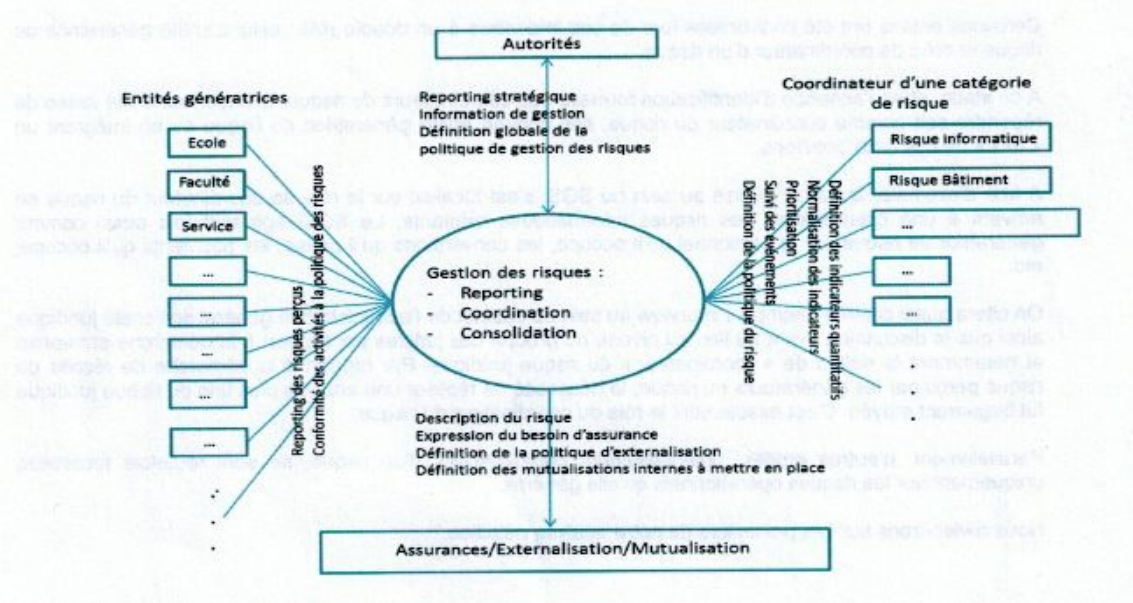


Figure 11: Gestion effective des risques [17]

La conclusion de l'étude donne des pistes pour l'implémentation d'un système de gestion des risques en éclairant l'institution sur la possible valeur ajoutée du projet. Deux éléments sont proposés, premièrement un reporting de la gestion des risques vers les autorités et deuxièmement un

[17] Source: *Gestion des risques - Etude exploratoire: risques perçus par les membres du CODIR*

support au processus d'externalisation des risques par le passage à une approche quantifiée.

4 Interviews des parties prenantes de l'Université catholique de Louvain

Une série de sept interviews a été réalisée auprès de différents directeurs et membres d'administration de l'UCL. Celles-ci ont été effectuées entre février et avril 2015 dans les locaux de l'UCL et se sont déroulées en français. La forme choisie a été celle des interviews face-à-face semi- structurées. Leur durée varie entre 30 et 60 minutes. Un test OCAI, servant à déterminer la culture existante et voulue de l'organisation, a également été proposé à la fin de l'entrevue. Les guides d'entretiens ainsi que le test OCAI sont disponibles en annexes [18]. La confidentialité des résultats a été garantie aux personnes interrogées pour leur permettre une plus grande liberté dans leurs propos.

4.1 Gestion actuelle des risques

Actuellement, il n'y a pas de gestion des risques de manière formelle à l'UCL. Chaque risque est géré de manière locale. Les directeurs d'administration sont amenés à gérer leurs risques de façon autonome, sans devoir rapporter ceux-ci ou leur gestion aux autorités supérieures.

Comme il l'a été indiqué dans la section 3, les risques ont été déterminés de manière spontanée. Selon l'auditeur interne de l'université, il peut y avoir des erreurs d'approximation de la part des différents directeurs, par exemple, à cause d'une myopie par rapport aux risques ou une habitude dans la gestion. Il manque donc une étape de validation. Selon l'auditeur, il faudrait une sorte de *"champion"* général du risque afin de gérer le risque de la manière la plus optimale possible. Il devrait être un coordinateur des différents risques de l'institution. D'autres intervenants mettent en garde sur l'importance de l'analyse du directeur qui est le plus à même de connaître et identifier ses propres risques. Le directeur du service d'étude insiste sur le manque d'un *"Monsieur Sécurité"*,

[18] Annexe 1,2 & 3 pour les guides d'entretien, Annexe 4 pour le test OCAI et Annexe 5,6,7,8,9 & 10 pour les verbatim

dont le rôle serait de vérifier la qualité et la pertinence de l'information.

Toutes les personnes interrogées reconnaissent que certains risques sont transversaux. Ils citent en général le risque informatique, dû à la gestion centralisée de ce dernier. Nombreux sont ceux qui ajoutent le risque de réputation, les plans d'urgences et/ou la gestion financière. Le directeur financier met en avant que la transversalité rend la gestion difficile vu que personne ne s'approprie les risques et ajoute qu'une gestion centralisée pourrait permettre d'éviter ce désagrément. Un des intervenants rajoute qu'il pourrait être intéressant d'utiliser les ressources et les savoirs présents à l'intérieur des facultés.

Lors de l'interview, il a été demandé d'identifier les différents fournisseurs de sûretés de l'université. Tous ont identifié l'audit interne et l'audit externe comme étant les principaux. De manière plus dispersée et moins systématique ont été cités parfois le *"groupe des juristes"*, la Cour des Comptes, les Commissaires du Gouvernement, l'administration financière, les différents conseils académiques (comme le conseil d'administration, le conseil d'audit ou le comité de gestion des ressources extérieures). Le département de gestion des risques n'existant pas, personne ne l'a identifié comme étant un fournisseur.

Les intervenants ont également donné leur avis sur les résultats de l'étude exploratoire. Cette initiative a été unanimement saluée, et leur a donné conscience des différents risques présents à l'UCL. Certains rajoutent que des risques qui ont été rapportés peuvent être sous-estimés du fait que les directeurs peuvent avoir une certaines myopie de leur risque. D'autres complètent qu'on ne peut savoir si les risques ont été quantifiés de manière optimale mais il appartient à l'UCL de les prendre en compte. Une partie des interviewés considère que certains départements ont exagéré dans l'évaluation de leurs risques. Le directeur des affaires étudiantes pense que les risques devraient être mieux arbitrés et harmonisés dans une centralisation renforcée.

4.2 Audit

Un service d'audit interne est présent à l'UCL. Il doit rapporter au comité d'audit qui est une émanation du Conseil d'Administration. Le comité d'audit est présidé par le président du CA

et contient un certain nombre d'administrateurs qui ne sont pas forcement membres de l'UCL. Le plan d'audit est principalement basé sur la légalité et la sauvegarde du patrimoine. Il est revu annuellement en collaboration avec le comité d'audit. Les standards édictés par l'IIA sont également respectés.

Selon l'auditeur interne, les missions actuelles du service d'audit sont au nombre de quatre.

- Réalisation d'audit tel que défini par le comité d'audit
- Contrôle des ASBL périphériques
- Contrôle des sociétés qui désirent s'implémenter dans le parc scientifique
- (Marginalement) les audits de fraudes, avis techniques demandés au niveau des services

Il est attendu de l'auditeur qu'il donne la température sur les procédés par son approbation ou sa désapprobation.

Les différents intervenants sont unanimement d'accord sur le respect de l'indépendance de l'auditeur. Cette dernière est légale et respectée dans les faits.

La plupart des personnes interviewées s'accordent sur le fait que l'auditeur n'est pas vu comme un inquisiteur mais plus comme un conseiller privilégié par son indépendance.

4.3 Projet d'implémentation

Comme il est dit plus haut, le projet d'implémentation vient d'un constat du département des risques et patrimoines de l'UCL. En effet, on ne peut s'assurer contre des risques indéterminés. De plus, le manque de centralisation de la gestion des risques est également un facteur de risques pour l'organisation. Le directeur du service d'étude considère cet outil comme très anglo-saxon et craint une surcharge de travail pouvant s'avérer inutile. Il considère que les risques présents dans les pays anglo-saxons et la mentalité varient fortement.

Une première étape a été réalisée en 2012 (finalisée en 2013) sous l'impulsion du directeur des risques et patrimoine. Cette première étape consistait principalement en une cartographie des risques des différentes entités du CODIR. Unanimement, cette initiative a été saluée par les personnes interrogées. Cette cartographie a également permis aux différents directeurs de se rendre compte des risques inhérents aux autres départements. Le directeur financier résume cette situation en déclarant que cette cartographie permet de mieux conscientiser les administrations aux risques de l'institution. Pour lui, il s'agit d'une valeur ajoutée qui permet d'éviter les déperditions financières. Par rapport à cette étude exploratoire, un des directeurs ajoute qu'il pourrait être intéressant de rajouter une dimension à cette cartographie, à savoir la vélocité d'apparition du risque.

Toutes les personnes interrogées sont conscientes de la valeur ajoutée qu'apporte la gestion des risques. Nombreux sont ceux qui considèrent que cette gestion des risques devrait permettre au management d'obtenir un meilleur fonctionnement de l'institution.

Les intervenants s'accordent sur la fonction de gestionnaire du risque. Elle devrait être, selon une des personnes interrogées, gérée par une personne de la même ligne hiérarchique que celle de l'audit interne. Le gestionnaire du risque devrait endosser le rôle de *"champion"* du risque en servant de coordinateur.

Trois des interviewés ont insisté sur la simplicité. Ils considèrent qu'un processus trop compliqué et trop invasif pourrait avoir plus d'effet négatif que positif. Un des directeurs ajoute qu'il ne faut surtout pas déresponsabiliser les individus en charge de la gestion des risques et donc les intégrer dans le processus.

Ce projet devrait, à la lumière des interviews, être conjointement géré par l'audit interne et par un département de gestion des risques. Le rôle de l'auditeur interne est de valider le processus. Celui du gestionnaire de risque est de couvrir, d'assurer les différents risques auxquels l'organisation fait face. Sa mission est à la fois tournée vers l'intérieur et l'extérieur. Le département devrait également servir de support aux différentes activités gérées. Son rôle est à la

frontière entre consolidateur des risques et *"champion"* des risques.

4.4 Culture et résultats OCAI

Le personnel administratif de l'université est affecté par les nombreux changements, ceux-ci pouvant être internes ou externes. Une certaine lassitude par rapport aux changements est palpable, surtout quand ceux-ci ne sont pas compris par les administrations.

Il est important d'insister sur le processus démocratique au sein de l'UCL. Ce mode de fonctionnement peut être selon un des intervenants une barrière à l'implémentation par une grande résistance au changement.

Un autre intervenant, présent à l'UCL depuis plus de 30 ans, remarque une perte de la *"patte UCL"*. Cette perte de culture interne est, selon lui, due aux recrutements extérieurs pratiqués par l'UCL. Cette démarche a l'avantage d'avoir une vision venant de l'extérieur mais a aussi pour conséquence une perte de la culture propre à l'université.

Nombreux sont les intervenants craignant le changement, qui est vu comme consommateur de temps. Une bonne information présentée de manière simple permet, selon un des interviewés, de lutter contre cette résistance au changement.

Les tests OCAI mettent en évidence que, dans la situation actuelle au sein de l'administration, la culture dominante est la culture de clan. La culture de marché est la culture la moins présente. Cet avis n'est cependant pas partagé par l'administrateur du site d'UCL Mons (ex-Fucam). Cette divergence d'opinion peut s'expliquer par la différence entre la situation actuelle et celle d'avant fusion. La culture adhocratique, arrivant en seconde place, semble infirmer le caractère flexible et discret de l'organisation.

Les résultats montrent également que la situation souhaitée par la plus grande partie des directeurs interrogés n'est pas fortement différente de la situation actuelle.

5 Analyse et recommandations

Le projet d'implémentation d'un ERM examine un processus épistémologique de détermination d'une situation de déficit de clarté pour qu'il soit adaptable à l'Université catholique de Louvain. Sur base de la théorie étudiée, nous allons tenter de donner nos analyses et nos recommendations. Le processus inité semble avoir été développé au départ d'une intuition. Le caractère positif consiste à avoir posé des hypothèses de travail. Il est toutefois regrettable, sans que cela ne soit ressenti comme une critique, de ne pas avoir déterminé des conditions de possibilités plus rationnelles et scientifiques lors des étapes préliminaires à l'implémentation. Le présent travail s'inscrit dans ce que le directeur du service des risques et patrimoines financiers a initié et essaie de déterminer la démarche scientifique à adopter afin d'examiner si l'université se trouve actuellement dans les conditions d'implémentation d'un ERM et, à défaut, de tenter de déterminer les conditions de changement préalables à une implémentation future.

Dans le cas de l'Université catholique de Louvain, la volonté d'implémentation ne provient pas d'une contrainte légale mais d'une réflexion de l'organisation pour rationaliser ses processus. Cette volonté trouve son origine dans une constatation du département des risques et patrimoine financier, ce dernier gérant notamment les polices d'assurance de l'université. En effet, une mauvaise appréhension des risques au sein de l'université ne permet pas de souscrire des polices d'assurance de manière efficiente. Ce processus d'externalisation des risques ne peut pas être réalisé pleinement sans connaissance préalable des risques présents en interne. Les autres parties prenantes de l'université ont également vu dans ce projet une certaine opportunité de bonne gouvernance par la possibilité de minimiser les déperditions financières et d'offrir au management une image fiable des risques assumés dans l'organisation afin de les aider à prendre une décision. L'absence d'ERM au sein de l'organisation est perçue par certaines parties prenantes comme en soi un risque supplémentaire. Lors des interviews, les intervenants ont émis certaines réserves par rapport au principe du projet d'implémentation. Premièrement, ils craignent qu'un ERM amène une certaine déresponsabilisation des parties prenantes.

> *Ca pourrait être comme dans certains de nos process où les gens se disent que "s'il y a un mort au bord de la route, ce n'est pas à moi de le ramasser".* (Interview° 4)

Deuxièmement, les intervenants ne veulent pas la mise en place d'un modèle identique à ceux des pays anglo-saxons qu'ils considèrent comme trop invasifs, trop complexes pour le cas de l'UCL. Ce dernier déclare:

> *On devrait rester à une formule plus souple* [...] *L'ERM est un outil très chronophage* [...] *très anglo-saxon où il faut tout croiser même quand c'est pas pertinant, parfois inutilement détaillé, c'est un peu comme la gestion des projets et la méthode PRINCE2.* (Interview^{o} 4)

Mis à part ces remarques, les différentes parties prenantes accueillent de manière favorable le projet. Initialement, ce projet visait à intégrer dans la gestion des risques l'ensemble de l'université par une gestion émanant uniquement des parties prenantes issues du CODIR, c'est-à-dire de la partie administrative de l'UCL. Les autres entités ne représentaient que 26% des risques cités lors de l'étude exploratoire bien qu'ils soient considérés de manière instinctive par les personnes interviewées comme étant les principaux générateurs de risques de l'organisation. Du fait que, dans la situation actuelle, la gestion des risques se réalise en silos et que les risques vécus ne soient pas rapportés aux autorités, de nombreux risques présents dans ces entités ne sont pas perceptibles par les membres du CODIR. Sans intégration de l'ensemble des parties prenantes de l'organisation, l'ERM pourrait s'avérer inefficace car du fait d'une mauvaise estimation ou d'une absence d'identification de certains risques.

> **Exemple:** Dans le cas où un laboratoire de recherche utilise un produit potentiellement dangereux sans en référer au management, celui-ci ne pourra prendre de mesure préventive pour atténuer les risques éventuels.

Le projet prend comme référentiel de base le guide COSO. Selon celui-ci, l'ERM possède des composantes interconnectées qui s'influencent mutuellement. Dans le cas où une des composantes n'est pas prise en compte ou tout au moins mal prise en compte, le projet pourrait ne pas être perenne. En analysant de manière détaillée la manière dont le projet a été mené jusqu'à présent, nous pouvons mettre en évidence que certaines étapes critiques du COSO ont été omises ou ont été réalisées de manière approximative. De plus, les différents rôles des parties prenantes n'ont pas été clairement définis au début du projet.

5.1 Environnement interne

L'étape de l'environnement interne, première étape du COSO, fait défaut lors de l'étude exploratoire. L'étude a directement débuté par l'étape d'identification des risques. Selon le COSO, l'impulsion de l'implémentation d'un ERM doit venir du management de l'organisation. Pour l'UCL, c'est le département des assurances et non le rectorat ou l'administration générale qui a initié le projet, même si ces derniers le soutiennent. Lorsqu'on analyse la culture de l'université, les tests OCAI montrent que la culture prépondérante au sein de l'administration est celle de clan. Ce type de culture est basé sur la coopération mais ne favorise pas la prise de risque au sein de l'organisation contrairement à une culture de marché. De plus, les intervenants insistent sur la résistance au changement et le processus démocratique (coûteux en temps) présent au sein de l'administration de l'UCL. Nous pouvons illuster l'exemple par l'intervenant n° 6:

> *L'université avec la sacro-sainte liberté académique, utilisée à toutes les sauces* [...] *l'université, est un milieu particulier et démocratique.*

Les tests OCAI n'ont pas été réalisés sur les autres entités de l'université, ce qui a pour conséquence de ne pas identifier avec certitude les autres cultures qui pourraient exister dans les entités non examinées. Les différentes personnes interviewées à ce jour insistent sur l'indépendance et la compétition pouvant exister en interne dans les entités périphériques. Dans celles-ci, selon les intervenants, on serait plus en adéquation avec une culture du risque. Ainsi il est déclaré:

> [...] *Bien souvent vous allez dans une entité, vous leur dites, vos voisins font comme ça et on voit qu'ils ne sont pas au courant de comment font les voisins et redéveloppent le même outil que celui existant à coté car je suis pas sûr que le voisin le donnerait* [...] *ils ne partagent pas.* (Interview° 5)

Lors des étapes préliminaires, les perceptions subjectives d'un certain nombre d'entités n'ont pas été analysées (facultés, instituts de recherches, spin-off, ...). L'efficacité du processus ne pourra être pleinement réalisé que par une prise en compte de l'ensemble de l'organisation (IIAbel & IRE, 2010) Nous considérons que des interviews et des tests complémentaires sur la culture organisationnelle devraient être réalisés afin de circonscrire la globalité de l'organisation. La sensibilisation aux risques doit devenir une priorité centrale dans la gestion de l'organisation. Selon

Sitkin et Pablo (1992), la culture d'entreprise doit être influencée par les leaders de l'organisation. Dans le cas de l'UCL, les intervenants considèrent qu'il existe deux structures agissant de manière parallèle et possédant chacune un leader différent, à savoir la partie administrative à travers l'administrateur général et la partie académique à travers le recteur. La culture du risque doit être insufflée par chaque leader en ce qui concerne son domaine d'intervention en tenant compte des subdivisions existantes à travers les DAF/DAS (pour les facultés), l'ADRE (pour les instituts de recherches) et les entités à autorités mixtes (hôpitaux, spin-off, ...) Les cultures dégagées de cette dynamique sont différentes et devraient en toute hypothèse être harmonisables pour implémenter un ERM global. Toutefois, si le but ultime est la synthèse, il n'en demeure pas moins que dans un premier temps opérationnel, chaque structure doit avoir son ERM le plus adapté à sa culture spécifique et qui peut être différent de l'un à l'autre. L'illustration 12 nous montre la dynamique pouvant être adoptée vis-à-vis des entités.

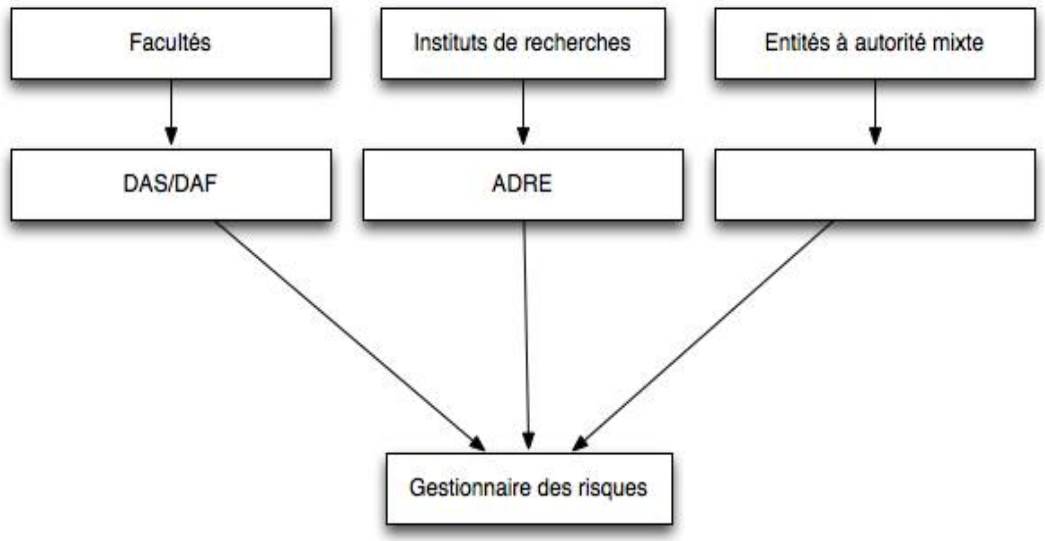


Figure 12: Dynamique de la gestion des risques par entités

Dans la situation actuelle, l'administration centrale est caractérisée par un fonctionnement très hiérarchique, un grand formalisme et aucun système de récompense. Selon Bozeman et Kingsley (1998), ce fonctionnement n'y favorise pas la culture du risque et pourrait être un frein à l'implémentation adéquate d'un ERM. Certains changements pourraient favoriser la culture du

risque et donc une bonne mise en place de l'ERM. L'organisation doit s'interroger sur le fait de savoir si elle repose sur une culture unifiée ou si ces différentes entités ont des cultures différentes. En fonction de la réponse qui sera donnée à cette problématique il faudra envisager une gestion de risques unique ou plusieurs gestions fragmentées autour des différentes cultures. Dans cette dernière hypothèse, un processus ultime de coordination doit être déterminé par exemple en la personne du champion du risque. Ce genre de gestion par paliers est déjà effectué dans certains établissements universitaires étrangers.

> **Exemple:**Au sein de l'Université de Cambridge, chaque département/école développe son ERM et le rapporte par la suite au département de gestion du risque qui consolide les informations à destination du management.

5.2 Identification des évènements

Après l'analyse de l'environnement interne, une autre étape aurait dû être analysée en amont de l'identification, à savoir l'étape de fixation des objectifs. Ceux de l'université sont clairement définis par décrets de la Fédération Wallonie-Bruxelles. En effet, la gestion des risques a pour but d'aider l'organisation à atteindre au mieux ses objectifs. Lors de l'étude exploratoire, nous avons pu noter que 63% des répondants n'ont pas défini les risques en relation aux objectifs poursuivis mais en fonction d'une interprétation subjective du risque qui leur était propre.

> **Exemple**:Le département CRCT (Cabinet du Recteur) définit le risque comme étant *"tout évènement, situation ou attitude dont on ne maîtrise pas les effets par méconnaissance ou manque d'expertise."*

L'étape d'identification des évènements a été la première réalisée par l'étude exploratoire. Cette dernière a uniquement été réalisée sur les membres du CODIR. La très grande majorité des risques identifiés ont été des risques opérationnels (82%). Les risques stratégiques (16%), structurels (1%) et étudiants (1%) n'ont été que fort peu cités par les différentes personnes interviewées. Les répondants ont donné leurs propres risques de manière spontanée et intuitive. Aucune identification des risques n'a été demandée aux entités extérieures au CODIR alors qu'elles sont, selon les intervenants, génératrices de la majorité des risques. Aucune recherche proactive des risques n'a

été réalisée et les risques multidimensionnels et transversaux n'ont pas été appréhendés. De plus aucune validation des résultats n'a été réalisée sur l'étude exploratoire par un vérificateur externe et indépendant aux départements interrogés. Alors que selon le COSO, une identification des risques doit se réaliser par une coordination des différentes fonctions de l'organisation. Dans les autres universités ayant déjà implémenté un ERM en leur sein, d'autres méthodes d'identifications ont été utilisées.

> **Exemple**: L'Université de Cambridge réalise, en plus des interviews traditionnelles, des séances de brainstorming, étudie les expériences du passé, les facteurs internes et externes et établit des hypothèses.

L'UCL peut s'inspirer des méthodes utilisées par les autres universités ou organisations similaires dans l'identification des risques ou définir ses propres méthodes, à son choix. Les avantages de la première alternative consistent à rendre plus rapidement opérationnel le processus d'implémentation et à se baser sur des méthodes déjà avérées, celles-ci pouvant s'adapter aux particularités et/ou aux besoins de l'UCL. Selon Green et Trieschmann (1984), une non-identification des risques rend les risques non-identifiables et donc le processus ERM non performant. L'étude exploratoire ne rencontre pas entièrement cette exigence. En effet, sans avoir d'image précise des risques présents, l'université pourrait rater l'implémentation de l'ERM (risques non identifiés, ressources mal allouées, ...). L'étude exploratoire a entraîné une sensibilisation à la gestion du risque mais doit être complétée par une description plus complète et plus scientifique des risques existants. Cette étude a permis malgré tout de mettre en exergue que certains responsables ont été sensibilisés dans leur propre département par les risques exposés ailleurs et ont de la sorte amélioré leur propre analyse des risques.

5.3 Evaluation des risques

Du point de vue de l'évaluation des risques, l'étude exploratoire se base sur la méthode traditionnelle proposée par le COSO, c'est-à-dire sur la fréquence d'apparition et sur l'importance relative des risques. Une cartographie des risques a été par la suite mise en place mais chaque entité a été analysée de manière séparée, ce qui a pour défaut de ne pas mettre en évidence les duplications nombreuses existantes.

Exemple: Le risque informatique est cité 17 fois dans les interviews.

Il manque également une étape de validation des résultats obtenus, les répondants ayant classé les risques de manière intuitive et non en fonction des objectifs. Certains intervenants ont par ailleurs marqué un étonnement sur le classement réalisé par d'autres entités. Un des intervenants déclare:

> *Chacun a une perception du risque qui est différente* [...] *mais quand BIUL* [19] *dit:"manque de personnel", c'est un risque* [...] *qui au risque de décevoir, si il y avait moins de personnel au niveau BIUL, on fermerait momentanément une bibliothèque.* (Interview° 3)

5.4 Traitement des risques

Dans l'étude exploratoire, un projet de traitement des risques a été proposé (voir section 4.3). Dans le processus proposé, le rôle de l'audit interne n'est pas pris en compte. Ce qui a pour conséquence que personne ne vérifie la cohérence de l'ensemble des processus de traitement des risques. Nous pouvons donc proposer une modification, comme présentée à l'illustration 13, en s'inspirant de ce qui se passe à l'Université d'Aberdeen par rapport à la première idée d'implémentation en donnant un rôle de vérificateur à l'auditeur interne de l'UCL.

Il manque également, comme l'indiquaient certaines personnes interviewées, une liste reprenant les compétences au sein de l'UCL. Cette liste existe seulement de manière parcellaire pour certaines fonctions bien précises (Groupe des juristes, Département de sécurité et radioprotection, ...). La création d'une liste de compétences faciliterait la nomination des coordinateurs d'une catégorie de risques comme le prévoit le plan d'action futur contenu dans l'étude exploratoire. L'université doit également définir son appétence aux risques et les actions à mettre en place, à savoir soit une acceptation, soit une diminution, soit une suppression, soit des plans d'action. De nombreux répondants à l'enquête liminaire indiquaient d'ailleurs dans leurs risques que l'absence de plans d'action appropriés était génératrice de risques.

[19] Bibliothèques de l'UCL

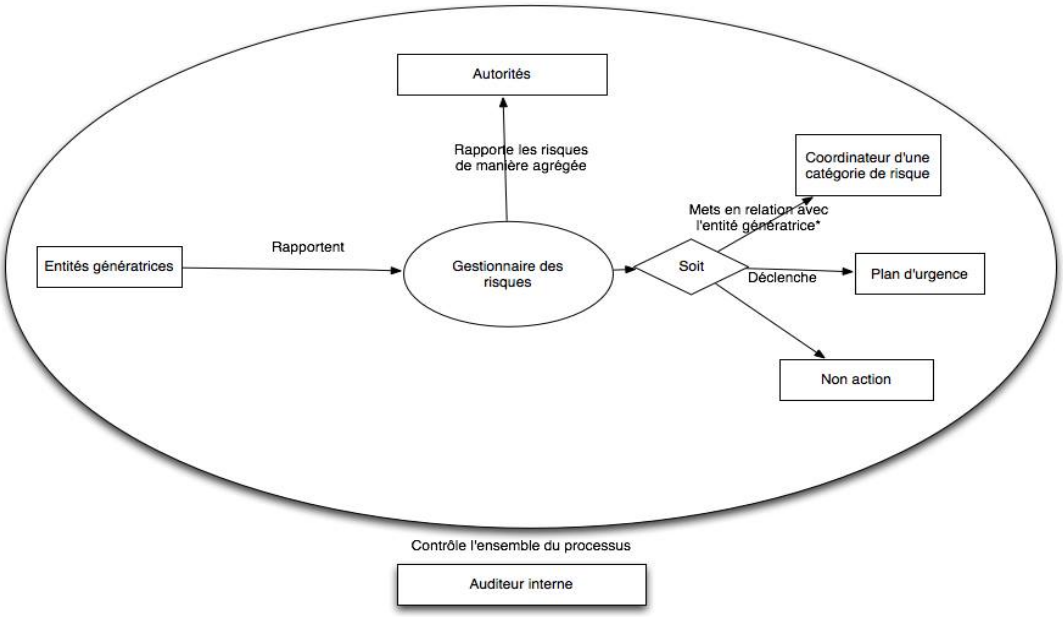


Figure 13: Gestion effective des risques

5.5 Activités de contrôles

La mise en œuvre d'un processus ERM implique que l'organisation contrôle l'ensemble des procédures et des mécanismes. Les agents chargés de cette mission peuvent a priori être l'auditeur interne et les gestionnaires de risques. L'université devra définir les modalités et la manière de réaliser les contrôles, tant au niveau global qu'au niveau des différentes entités.

5.6 Informations et communications

Tant la recherche des risques que les mécanismes de contrôles impliquent un langage performatif commun et la communication de l'ensemble des procédures et politiques vers les parties prenantes. La création de ce type de document peut s'inspirer de ce qui est réalisé dans les universités anglo-saxonnes. En annexe 11, un exemple de plan et procédure issu de l'Université d'Aberdeen est produit à titre d'illustration. Selon Coetzee et Lubbe (2014), un langage universel sur la gestion des risques n'existe pas à l'heure actuelle. Il appartient dès lors aux organes moteurs du projet (audit, gestion du risque, ...) de définir ce langage qui englobe tant la dimension sémantique (fond) que syntaxique (forme). Ainsi, la création d'un langage commun par l'ERM

mène à une amélioration de la communication au sein de l'organisation (Acharya, 2009). Cette volonté d'amélioration de la communication est exprimée par un des interviewés pour les sites universitaires situés en dehors des communes d'Ottignies-Louvain-la-Neuve et de Woluwe-Saint-Lambert. Ce dernier déclare:

> [...] *Pour la gestion de nos risques, on demande à ce que Louvain nous entende* [...] *ce qui n'est pas le cas dans la situation actuelle.* [...] *il y a un véritable problème de communication entre nous et Louvain.* (Interview^{o} 3)

Ce langage devra par la suite être communiqué et expliqué à l'ensemble des parties prenantes de l'université. Pour ce faire, les conditions de possibilités devront être analysées en concertation avec les départements de communication (AREC) et de l'information (SGSI). De plus, une gestion efficace implique une définition commune du risque orientée vers les objectifs. Le COSO a émis des définitions (du risque et de la gestion du risque) qui peuvent être utilisées pour l'implémentation et communiquées aux différentes parties prenantes. Le gestionnaire du risque devra également communiquer les principaux résultats au management de l'université. Dans ce cadre, il peut être utile qu'un rapport complet soit transmis au management mais accompagné d'une synthèse mettant en évidence la substance des informations communiquées. Comme le met en évidence Mckinsey & Company (2010), le rapport doit se concentrer sur l'essentiel des informations qui puissent être comprises et digérées par le management. L'auditeur interne de l'université a d'ailleurs insisté dans son interview sur le fait que ses rapports d'audit actuels étaient plus concis que ceux de son prédécesseur, ceci est la preuve que la démarche de transmission de rapport doit s'axer sur l'essentiel.

5.7 Pilotage

Bien qu'aucun élément de l'ERM ne puisse être considéré comme plus important que l'autre, la phase de pilotage est celle qui permet à l'ensemble de la dynamique de faire corps (Nelson et Ambrosini, 2007). L'ERM est un processus dialectique impliquant un devenir de l'implantation eu égard à son développement. L'UCL devra sur une base régulière réviser l'avancée de l'implantation. Power (2009) met ainsi en évidence que les modifications du processus doivent se faire sur les erreurs du passé et les changements d'environnement interne et externe. L'université

doit définir les méthodes de pilotage en coordination avec les différents acteurs de l'institution. Cette phase doit s'étendre dans le temps avec des moments spécifiques de révision de la même manière que dans les autres universités ayant déjà implémenté l'ERM.

> **Exemple**: Dans son plan de gestion des risques, l'Université d'Aberdeen prévoit de revoir en profondeur son plan tous les trois ans.

5.8 Rôles et responsabilités

Du point de vue des rôles et responsabilités, la charge première en incombe au Management (COSO, 2004). Dans les faits, la question se pose de la délégation. Selon l'étude de Christopher et Sarens (2015) portant sur la gestion des risques dans les universités australiennes, l'implémentation peut être réalisée par plusieurs départements différents, soit par le département d'audit interne, soit par un département de gestion des risques ou soit par une externalisation de la gestion des risques. Le projet semble se porter pour la gestion des risques sur un département interne autre que celui de l'audit, à savoir la création d'un nouveau département spécialisé dans la gestion des risques. Lors des travaux préparatoires, l'importance de l'auditeur interne semble avoir été minimisée dans la phase d'implémentation. L'étude exploratoire considère que l'auditeur n'a pas de responsabilité dans l'implémentation première. La responsabilité revenant en premier lieu au gestionnaire du risque. Or, selon la définition de l'IFACI (2000), l'indépendance et l'objectivité de l'auditeur interne permettent de donner à l'organisation une sûreté sur le degré de maîtrise de ses opérations. Ce rôle de vision générale dans son indépendance donne à l'auditeur interne une place centrale dans le processus qui n'a pas été utilisée suffisamment. Il aurait été adéquat que ce dernier soit impliqué dès le départ dans ce cheminement. Les tâches qui sont réservées à l'auditeur interne selon l'IIA sont les suivantes :

- Donner la sûreté sur le processus de gestion du risque
- Donner la sûreté que les risques sont correctement évalués
- Evaluer le processus de gestion des risques
- Evaluer le rapport sur les risques principaux

- Revoir la gestion des risques principaux

Les tâches susmentionnées ne peuvent être soustraites à la responsabilité de l'auditeur interne. D'autres tâches ne peuvent en aucun cas être réalisées par l'auditeur interne afin de préserver son indépendance :

- Définir l'appétit pour le risque
- Imposer le processus de gestion des risques
- Gérer la sûreté sur les risques
- Prendre les décisions sur les réponses à apporter aux risques
- Implémenter une réponse aux risques au nom du management
- Prendre la responsabilité pour la gestion des risques

Ces tâches doivent revenir au gestionnaire du risque sous la responsabilité finale du Management de l'organisation. Les autres fonctions de la gestion des risques doivent faire l'objet de négociation entre le département d'audit et le département de gestion des risques. Cette zone grise comprend les tâches suivantes :

- Faciliter l'évaluation et l'identification des risques
- Coacher le management dans la réponse à apporter aux risques
- Coordonner les activités ERM
- Consolider le rapport sur les risques
- Maintenir et développer un cadre pour l'ERM
- Etre un champion dans la mise en œuvre de l'ERM
- Développer une stratégie de gestion des risques pour l'approbation par le Management

Etant donné que selon le COSO (2004) la responsabilité principale de la gestion des risques est détenue par le management, il appartiendra à celui-ci de faire l'arbitrage qui lui apparaitra le plus opportun pour la zone grise eu égard aux qualifications, aux compétences et à la disponibilité des parties prenantes. Si l'UCL veut se diriger vers la solution du gestionnaire du risque, elle doit veiller à ce que celui-ci ait la signalétique suffisante et à défaut qu'une formation complémentaire soit acquise par celui-ci. Une attention toute particulière doit être réservée au champion du risque, ce dernier doit posséder certaines caractéristiques. Selon l'IIA (2009), le champion doit éduquer les parties prenantes et insuffler la volonté au sein de l'ensemble de l'organisation. Ce champion pourrait être la personne qui a initié le travail préparatoire. La présence d'un champion du risque augmentera de manière considérable la bonne implémentation de l'ERM (Beasley et al. , 2005). De plus, certains changements devront également apparaître dans la manière de réaliser les audits à l'université. Dans la situation actuelle, les audits sont basés sur la légalité et la sauvegarde du patrimoine. Dans le cas d'un ERM, l'audit devra également prendre en considération le risque.

Les éléments ci-dessus résultent d'une position de l'IIA et non d'une norme obligatoire. Il en découle qu'il n'y a pas de caractère légal en Belgique même si son respect est fortement conseillé. Nous attirons l'attention du management sur la nécessité de tenir compte du rôle minimal de l'auditeur interne et en fonction des compétences des différents protagonistes leur attribuer les tâches les plus adéquates. Il va de soi que les personnes choisies devront suivre les formations requises comme par exemple celles proposées par l'IRM. Ces formations sont disponibles en ligne et peuvent être suivies directement en *streaming*.

5.9 Valeurs ajoutées

Dans la situation actuelle, il n'y a aucune contrainte légale pour l'implémentation d'un processus de gestion des risques au sein des universités en Fédération Wallonie-Bruxelles. La recherche de valeur ajoutée est donc l'élément déterminant à l'implémentation. L'élément central de la gestion des risques doit être de permettre à l'organisation d'atteindre ses objectifs de la manière la plus efficiente possible (COSO, 2004). Dans le cas de l'UCL, cette gestion des risques devra se faire en fonction des objectifs suivants ; l'enseignements, la recherches et les missions à la société.

Au regard des interviews, la plupart des intervenants ont considéré qu'il y avait une valeur

ajoutée sans être précis sur celle-ci. Par exemple, un des interviewés déclare à propos de cette valeur ajoutée :

> *Il y aura sûrement une valeur ajoutée* [...] *une stucture qui permet de mieux mesurer ne peut être que positive.* (Interview n^{o} 2)

D'autres mettent en avant certains avantages d'une telle implémentation :

- Uniformisation de la gestion des risques
- Coordination des risques au sein de l'université
- Avantage concurrentiel
- Rationalisation des polices d'assurances
- Meilleure conscientisation des départements aux risques
- Amélioration des procédures

L'étude exploratoire a également mis en évidence que l'absence de plan d'urgence est ressentie comme un manque pour la gestion de l'université. En ce qui concerne l'étude réalisée sur des compagnies d'assurances (Grace, Leverly, Philips et Shimpi, 2010), il a été démontré que l'implémentation d'un ERM a entraîné une rationalisation de l'efficacité de leurs coûts. Mais selon l'étude effectuée par Mckinsey & Company (2010) la manière dont l'ERM est construit est capitale pour la recherche de valeurs ajoutées. Ces deux références nous montrent que de manière empirique, la plus-value est possible mais n'est pas automatique. Pour obtenir une valeur ajoutée, ce qui doit être le but recherché, certains éléments doivent être mis en évidence (Mckinsey & Company, 2010):

- Axer son action sur la valeur ajoutée
- Se concentrer sur un petit nombre de risques clés ayant des gains et des pertes disproportionnés
- Optimaliser la préoccupation sur les risques

- La gestion des risques doit être centrale pour les décisions stratégiques et opérationnelles
- La fonction doit être mise en exergue, facilitée par une personne hautement qualifiée

La préoccupation aux risques doit être toujours présente à l'esprit du management, de l'audit interne et du gestionnaire du risque avec une coordination au niveau de la sensibilité par le champion du risque. Pour obtenir une valeur ajoutée optimale, le gestionnaire des risques ne doit pas se contenter d'une attitude minimaliste mais doit ambitionner l'achèvement du projet dans ses buts ultimes. L'université doit définir en amont de cette gestion les avantages qu'elle recherchera à travers la gestion des risques.

5.10 Messages et découvertes principales

Lorsqu'est analysé le projet tel que mené jusqu'à présent, voici, à notre estime, les problèmes principaux qui en résultent. Si l'université désire mettre en oeuvre un processus ERM efficient, cette dernière devra prendre en considération les points suivants:

- Culture inadéquate au sein de l'administration
- Culture hétérogène au sein de l'organisation
- Résistance aux changements de la part des parties prenantes
- Mauvaise identification des risques lors de l'étude exploratoire
- Manque de précision dans le processus de traitement des risques
- Manque de validation des résultats lors de l'étude exploratoire
- Problème de communication en interne
- Détermination des rôles dans le processus
- Détermination de la valeur ajoutée imprécise

Tant que ces éléments n'ont pas trouvé réponse, une implémentation d'un ERM anticipée est vouée, nous semble-t-il, à l'échec.

Conclusion

Stratégie pour l'implémentation d'un ERM à l'UCL : utopie ou réalité ? L'implémentation, comme nous l'avons vu, a ses règles. Dans la partie théorique, nous avons déterminé les conditions de possibilités d'une implémentation selon le référentiel du COSO : le respect des étapes interconnectées et des rôles et responsabilités de chacune des parties prenantes. Les étapes sont les suivantes :

- Environnement interne
- Détermination des objectifs
- Identification des risques
- Evaluation des risques
- Traitement des risques
- Contrôle
- Information et communication
- Pilotage

Les rôles et responsabilités dans le cadre de ces étapes ont été déterminés. Selon le COSO, la responsabilité finale incombe au management de l'organisation avec délégation des fonctions exécutives vers d'autres départements, internes et/ou externes. L'auditeur interne joue un rôle obligatoire au moins minimum [20] dans l'exercice de ses fonctions, peu importe le choix opéré par le management. Dans le cas où la fonction est réalisée par un gestionnaire du risque ou un département externe, un arbitrage devra être effectué par le management entre ses fonctions et celles de l'auditeur interne.

Ce mémoire après avoir rappelé les conditions théoriques d'une implémentation d'un ERM dans le cadre des organisations a tenté d'appliquer celles-là au cas particulier de l'UCL. Nous

[20] cfr demi-cercle de l'IIA

sommes partis de l'étude exploratoire réalisée récemment et avons poursuivi une réflexion qui a voulu déboucher sur une éventuelle concrétisation pratique au départ d'une théorie générale.

Le département des risques et assurances de l'UCL a voulu sensibiliser celle-ci sur les avantages d'une implémentation à travers une étude exploratoire. Cette recherche est partie d'une intuition que la gestion des risques par silos et en bon père de famille n'optimalise pas les résultats qui pourraient être attendus. Cette manière d'appréhender la problématique nous paraît insuffisante. L'organisation que constitue l'UCL est multiple. Incontestablement, des parties importantes et significatives n'ont pas été examinées avec toute l'attention nécessaire. N'oublions pas que tous les acteurs qui devront être impliqués dans l'implémentation ne sont pas uniquement les membres du CODIR mais l'ensemble du personnel de l'UCL. Si ces personnes ne sont pas impliquées activement dans le processus, alors celui-ci ne pourra pas aboutir à un dynamisme suffisant.

Nous avons développé dans la partie pratique une critique de cette approche et ouvert des perspectives positives pour une implémentation future au sein de l'UCL. La question qui mérite d'être approfondie consiste à savoir si une culture commune peut être partagée par les différentes entités et sites de l'UCL. Cette approche n'a pas encore été réalisée et est préalable à toute avancée ultérieure. Une implémentation qui ferait l'économie de cette étape manquerait de fondement solide. Pour la plupart des personnes interviewées, leur intuition et connaissance empirique les ont amenées à considérer la coexistence de plusieurs cultures distinctes au sein de l'UCL. Une gestion du risque unifié, en tout cas dans un premier temps organisationnel, semble illusoire. Sous réserve des résultats de l'étude complémentaire suggérée, une gestion des risques par paliers nous semble être préconisée mais le but de l'harmonisation doit rester présent à l'esprit du management à travers un rôle central à décerner au champion du risque. En ce qui concerne plus particulièrement le CODIR, il importe que le risque soit axé davantage sur les objectifs et qu'une sensibilisation aux risques soit plus présente dans la culture de l'organisation.

Il sera déterminant de considérer cette implémentation comme un changement. Tout changement doit être préalablement analysé pour s'assurer du bon déroulement de ce dernier. La revue

de littérature du mémoire donne quelques pistes d'analyses (Kotter, 1995, Lattier, 2015). D'autres théories (Lewin, 1947; Bareil & Savoie, 1999) pourront être examinées pour optimaliser les bonnes conditions du changement. Un test OCAI a été proposé lors des interviews réalisées. Ce dernier, disponible à l'annexe 4, pourra être utilement soumis aux entités non encore examinées afin d'en déterminer la culture, étape liminaire à l'implémentation d'un ERM.

A l'exception de l'étape de l'environnement interne, les autres phases du processus ne devraient pas poser de problèmes insurmontables. Il convient que les personnes chargées de ces missions, à savoir l'auditeur interne et le gestionnaire des risques, aient les compétences et les formations requises.

Il résulte de ce qui précède qu'un travail préparatoire doit compléter l'étude exploratoire initiale. Dans l'entretemps, l'implémentation ne peut pas débuter car les conditions de possibilités ne sont pas encore réunies. En effet, aucune identification substantielle des risques n'a été réalisée, les cultures restent toujours indéterminées, les rôles à remplir par les parties intervenantes ne sont pas clarifiés et les arbitrages entre les différents acteurs font défaut. Si l'organisation fait le choix d'opter pour la réalisation d'une phase préparatoire telle que suggérée ci-avant, les résultats de cette étude pourraient permettre d'examiner si une implémentation unifiée est tout d'abord possible et si elle peut apporter une valeur ajoutée. Dans l'état actuel de la législation, aucune obligation décrétale n'existe. La seule justification pour implémenter un ERM réside dans la valeur ajoutée qui serait éventuellement découverte.

Les tâches préparatoires sont importantes et ne peuvent être éludées. Nous conseillons au management et aux parties prenantes de prendre en compte et d'approfondir les éléments présentés à la partie 5.10 de la partie pratique.

Au terme de ce travail, deux questions apparaissent comme centrales pour la détermination de l'utilité à investir dans l'implémentation d'un ERM à l'UCL, à savoir l'environnement interne et la valeur ajoutée. Ces deux éléments me semblent être les difficultés du projet. En ce qui concerne la valeur ajoutée, la simple meilleure gestion des polices d'assurance est insuffisante pour justifier à

elle-seule la mise en place de l'ERM. La diversité des cultures qui devrait probablement apparaître complexifie l'implémentation envisagée.

Cette conclusion peut apparaître quelque peu pessimiste mais ouvre malgré tout des perspectives futures sans pour autant s'engager trop rapidement dans un processus coûteux et aléatoire. Utopie ou réalité ? Ni l'une, ni l'autre. Actuellement une implémentation d'un ERM à l'UCL est prématurée. Mais vu la possibilité d'un apport concurrentiel au profit de l'organisation dans le cadre d'un marché de plus en plus rigoureux, la démarche suggérée d'une étude complémentaire ne doit pas être écartée, bien au contraire.

Ce mémoire a étudié un processus d'implémentation d'un ERM au sein d'une université située en Europe Continentale, ce qui a été rarement réalisé. Il a été rédigé en français, bien que la quasi-totalité des sources soit en anglais, afin d'être plus accessible à son public cible.

A mon sens, une gestion des risques formalisée pourrait, dans le cas d'une implémentation efficace, donner un avantage concurrentiel non négligable à l'université par rapport à ses concurrents. Ce processus peut apporter une efficacité pour l'UCL dans son ensemble par une plus grande cohérence, une rationnalisation des processus et une aide à la décision. Un ERM permet également de préparer l'organisation étudiée aux différents changements externes qui pourraient subvenir. Implémenter un tel processus pourrait en plus donner un goût dans les nouvelles méthodes de management et entraîner une dynamique d'innovation. De plus, l'ERM pourrait être rendu obligatoire dans la prochaines années, comme aux Etats-Unis et en Grande Bretagne. La préparation de cet ERM constituerait une attitude proactive.

"Seuls ceux qui prennent le risque d'échouer spectaculairement réussiront brillamment" (John F. Kennedy).

Bibliographie

- Acharya, V.V. (2009). A theory of systemic risk and design of prudential bank regulation. *Journal of Financial Stability*, 5, 224-255.
- Adda, J. (2007). *La mondialisation de l'économie.* Paris: La découverte.
- Arena, M., Arnaboldi, M., & Azzone, G. (2010). The Organizational Dynamics of Entreprise Risk Management. *Accouting Organizations and Society*, 659-675.
- Aubry, C. (2012). La naissance de la fonction "risk manager" en France. *Management & Avenir*, 55, 14-35.
- ASX Corporate Governance Council (2007). *Corporate Governance Principles and Recommendations*. Australia: Corporate Governance Council.
- Baily, C.W.,& Petersen, D. (1989). Using Safety Survey to assess Safety System Effectiveness. *Professional Safety*, 2, 22-26.
- Baker, N. (2009). *A new direction, Internal Auditor.* `http://www.theiia.org/intAuditor/free-feature/2009/december/a-new-direction/` (consulté le 11/07/2015).
- Bareil, C.,& Savoie, A. (1999). Comprendre et mieux gérer les individus en situation de changement organisationnel *Gestion, revue internationale de gestion*, 24 (3), 86-94.
- Beasley, M.S., Clune, R.,& Hermanson, D.R. (2005). Enterprise riskmanagement: An empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy*, 24 (6), 521-531.
- Bozeman, B.,& Kingsley, G. (1998). Risk culture in public and private organizations. *Public Administration Review*, 58(2), 109-118.
- Bookstaber, R. (1999). Risk Management in Complex Organizations. *Presentations given to the Berkeley Finance Symposium and the Federal Reserve Bank of Atlanta Risk Management Conference*, Altanta.

- Burkett, V., Suarez, A.G., Bindi, C., Conde, M. Mukerji, Prather, R., St.Clair, A.L.,& Yohe,G. (2014). *Impacts, Adaptation, and Vulnerability. Contribution of Working Group II to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change.* Cambridge & New York: Cambridge University Press.

- California Technology Institute (2015). *Risk Management*. `http://www.admin.cam.ac.uk/offices/secretariat/risk/` (Consulté le 17/04/2015).

- Cadbury, A. (1992). *Report of the Committee on the Financial Aspects of Corporate Governance*, Londres: GEE.

- Cameron, K.S.,& Quinn, R.E. (2006). *Diagnosing and changing organizational culture: Based on the competing values framework.* San Francisco: Jossey-Bass.

- Chartered Enterprise Risk Actuary (2009). The Financial Crisis-the CRO Forum's Views on the Consequences for Enterprise Risk Management and Regulation in the Insurance Industry. *Risk Management*, 15, 3-45.

- Christopher, J.,& Sarens, G. (2015), Risk Management: Its Adoption in Australian Public Universities within an Environment of Change Management – A Management Perspective. *Australian Accounting Review*, 25(1), 1-12.

- Coetzee, P.,& Lubbe. D. (2014). Improving the Efficiency and Effectiveness of Risk-Based Internal Audit Engagement. *International Journal of Auditing*, 18(2), 115-125.

- Committee of Sponsoring Organisations of the Treadway Commission.(2004). *Enterprise Risk Management - An Integrated Framework*. New York: COSO.

- Courtot, H. (1998). *La gestion des risques dans les projets*. Paris: Economica.

- CS Star (2006). *Risk and Claims Management*. New-York: CS Star LLC.

- Douglas, M. (1999). *Implicit Meaning*. Londre: Routledge.

- Denman, B.D. (2005). *Comment définir l'université du XXIéme siécle?*. OECDilibrary, 17 (2), 9-30.

- Federation of European Risk Management Association (2002). Cadre de référence de la gestion des risques. http://www.ferma.eu/app/uploads/2011/11/a-risk-management-standard-french-version.pdf (consulté le 11/07/2015).

- Fédération Wallonie-Bruxelles (2015). *Textes Fondamentaux*. http://www.enseignement.be/index.php?page=25230 (Consulté le 10/04/2015).

- Financial Stability Board (2009). *Risk Management Lessons from the Global Banking Crisis of 2008*, http://www.financialstabilityboard.org/publications/r_0910a.pdf (consulté le 11/07/2015).

- Fralinger, B.,& Olson, V. (2007). Organizational Culture at The University Level: a Study Using the OCAI Instrument. *Journal of College Teaching & Learning*, 4(11), 85-98.

- Grace, M.F., Leverty, T., Phillips, R.D. & Shimpi, P. (2015). The Value of Investing in Enterprise Risk Management. *Journal of Risk and Insurance*, 82(2), 289-316.

- Green, M.R.,& Trieschmann, J.S. (1984). *Risk and Insurance*. Cincinati: South Western Publiching Co.

- Harrington,S.E.,& Niehaus, G. (1999). Basis risk with PCS catastrophe insurance derivative contracts. *Journal of Risk and Insurance*, 66, 49–82.

- HCCA Audit & Compliance Committe Academy (2011). *Risk Assessement and Internal Controls*. http://fr.slideshare.net/theHCCA/risk-assessments-internalcontrolsnueske (Consulté le 23/04/2015).

- Head, G.L.,& Horn, S. (1997). *Essentials of Risk Management*. New York: Insurance Institute of America.

- Higgs Report (2003). *Review of the role and effectiveness of non-executive directors*.Londre: Stationery Office

- Hoffman, D.G. (2002). Managing Operational Risk: 20 Fime-Wide Best Practice Strategie. New-York: John Winley.

- Insitut Français de l'Audit et du Contrôle Interne (2000). *Définition de l'audit interne.* `http://www.ifaci.com/` (Consulté le 2/07/2015).
- International Organization for Standardization (2009). *ISO 31000:2009, Management du risque – Principes et lignes directrices*. Londre: ISO.
- Jorion, P. (2008). *La crise. Des subprimes au séisme financier planétaire*. Paris: Fayard.
- Landsittel, D.T.,& Rittenberg, L.E. (2010). COSO: Working with the Academic Community. *Accounting Horizons*24(3), 455-469.
- Latier, M. (2015). *LSMF2007 - Gestion du Changement*. Ottignies-Louvain-la-Neuve: Université catholique de Louvain.
- Larousse (2008). *Larousse illustré 2009*. Paris: Larousse.
- Leclerq, J.M. (1999). *L'éducation comparée: Mondialisation et spécificités francophones*. Paris : CNPD.
- Lenz, R.,& Sarens, G.(2012). Reflections on the Internal Auditing Profession: What Might Have Gone Wrong". *Managerial Auditing Journal*, 27(6), 532-549.
- Lewin, K. (1947). Frontiers in Group Dynamics. *Human Relations*, 1(5), 5-41.
- Kaliprasad, M.(2006). Proactive Risk Management. *Cost Ingineering*, 48(12), 26-36.
- Kallman, J.,& Maric. R.V. (2004). A Refined Risk Management Paradigm. *Risk Management*, 6(3), 57-68.
- Kehm, B.,& Lanzendorf, U. (2006). The Impacts of University Management on Academic Work: Reform Experiences in Austria and Germany. *Management Review*, 18(2), 153-173.
- Kleffner, E., Lee, B.R.,& McGannon, B. (2003). The Effect of Corporate Governance on the Use of Enterprise Risk Management: Evidence From Canada. *Risk Management and Insurance Review*, 6(1), 53-73.
- KPMG (2007). *The Evolution of Risk and Controls: from Score-Keeping to Strategic Partnering*. Switzerland: KPMG.

- KPMG. (2010) *Reconceptualizing the Determinants of Risk Behavior.* Amsterdam: KPMG International.
- Kotter, J.P. (1995). Leading Change : Why Transformation Effort Fail. *Harvard Business Review*, 1-10.
- Nelson, M.,& Ambrosini, J. (2007). Enterprise Risk Management and Controls-Monitoring Automation Can Reduce Compliance Costs. *Bank Accounting & Finance*, 25-30.
- Niamh, B.,& Solomon, J. (2008). Corporate Governance and Mechanisms of Accountability : An Overview. *Auditing, Accountability Journal*, 21(7), 885-906.
- NYSE Listing Standard (2013). *Corporate Governance Standards.* `http://nysemanual.nyse.com/LCMTools/PlatformViewer.asp?selectednode=chp_1_4_3&manual=%2Flcm%2Fsections%2Flcm-sections%2F` (Consulté le 18/03/2015).
- McKinsey & Company (2008). *Making Risk Management a Value-adding Function in the Boardroom*. New York: McKinsey & Company.
- McKinsey & Company (2010) *A Board Perspective on Risk Management*. New York: McKinsey & Company.
- McNamee, D.,& McNamee, T. (1995). The Transformation of Internal Auditing. *Managerial Auditing Journal*, 10(2), 34-37.
- Morgan, G. (1979). The Internal Control Exposion. *International Journal of Auditing*, 5(2), 160-170.
- Morphew, C., & Hartley, M. (2006). Mission statements: A thematic analysis of rhetoric across institutional type. *The Journal of Higher Education*, 77(3), 456-471.
- Organizational Culture Assessment Instrument, (2005). *Making your OCAI-online*. `http://www.ocai-online.com/` (Consulté le 21/04/2015).
- Pesqueux, Y. (2011). Pour une épistémologie du risque. *Management & Avenir*, 3(43), 460-475.

- Power, M. (2007). *Organized uncertainty: Designing a world of risk management.* Oxford: Oxford University Press.
- Power, M. (2009). The Risk Management of Nothing. Accounting, Organizations and Society, 34, 849–855.
- PricewaterHouseCooper(2012). *Break-out Risk Management Commodity Trading No longer just for the traders!* Royaumes-Unis: PricewaterHouseCooper.
- Proviti, TNS, Sofres & l'Expansion (2004). *Baromètre du Risk Management*. `http://www.consultingnewsline.com/Info/Etudes%201/Barometre%202004.pdf` (Consulté le 14/03/2015).
- Pritchett, S.T., Schmit, H., Doerpinghaus, I.,& Athearn J.L.(1996).*Risk Management and Insurance*. Cincinati: South Western Publiching Co.
- Rejda, G. E. (1998). *Principles of Risk Management and Insurance.* New York: Sixth Edition.
- Rombouts, M.(2013). *Gestion des risques - Etude exploratoire: risques perçus par les membres du CODIR*. Ottignies-Louvain-la-Neuve: Université catholique de Louvain.
- Scott, P. (1998). *Massification, Internationalization and Globalization: "The Globalization of Higher Education"*, Buckingham: Open University Press.
- Shaw,J.(2005). Managing All your Enterprise's Risks. *Risk Management*, 52(9), 22–30.
- Sitkin, B.,& Pablo, A. (1992). Reconceptualizing the Determinants of Risk Behavior. *The Academy of Management Review*, 17(1), 9-38.
- Spira, L.F.,& Page, M. (2003). Risk management: The reinvention of internal control and the changing role of internal audit. *Accounting, Auditing & Accountability Journal*, 16(4), 640 - 661.
- Stroh, P.J. (2005). Enterprise Risk Management at United Healthcare. *Strategic Finance*, 27-35.

- Stulz, R.M. (2008). Risk Management Failures: What are They and When do They Happen?. *Fisher College of Business Working Paper*.

- Taylor, J.B. (2008). *The Financial Crisis and the Policy Responses: An Empirical Analysis of What Went Wrong*. `https://web.stanford.edu/~johntayl/FCPR.pdf` (consulté le 11/07/2015).

- Tchankova, L. (2002). Risk identification – basic stage in risk management. *Environmental Management and Health*, 13(3), 290 – 297.

- The Institute of Internal Auditors (2004). *Internal Auditing and ERM: Fitting in and Adding Value*. Altamonte Springs: The Institute of Internal Auditors.

- The Institute of Internal Auditors (2009).*The Role of Internal Auditing in Enterprise-Wide Risk Management.* Altamonte Springs: The Institute of Internal Auditors.

- The Institute of Internal Auditors (2012). *International Standards for the Professional Practice of Internal Auditing*. Altamonte Springs: The Institute of Internal Auditors.

- The Institute of Internal Auditors Belgium & Institut des Réviseurs d'Entreprises (2010). *Assurance externe versus assurance interne: Comment créer une coopération?* Bruxelles: The Institute of Internal Auditors Belgium & Institut des Réviseurs d'Entreprises.

- The Institute of Risk Management (2015). *Professional Standard.* `https://www.theirm.org/` (Consulté le 24/04/2015).

- Université catholique de Louvain (2015). *Site de l'Université catholique de Louvain.* `https://www.uclouvain.be/` (Consulté le 13/04/2015).

- University of Aberdeen (2015). *Risk Management*. `http://www.admin.cam.ac.uk/offices/secretariat/risk/` (Consulté le 17/04/2015).

- University of Cambridge (2015). *Risk Management*. `http://www.admin.cam.ac.uk/offices/secretariat/risk/` (Consulté le 17/04/2015).

- University of Denver (2015). *Entreprise Risk Management*. `http://www.admin.cam.ac.uk/offices/secretariat/risk/` (Consulté le 17/04/2015)

- University of Pretoria (2015). *Risk Management and Internal Audit*. `http://www.up.ac.za/risk-management-and-internal-audit` (Consulté le 14/04/2015).

- Walker, P.L., Shenkir ,W.G.,& Barton, T. L. (2002). *Making Enterprise Risk Management Pay Off*, Upper Saddle River: Ftpress.

- Williams, J.R., Young, P.C.,& Smith, M.L. (1998). *Risk Management and Insurance*. New York: McGraw-Hill/Irwin.

- Yazid, A., Razali, A.,& Hussin, I. (2012). Determinants of enterprise management: A proposed framework for Malaysia public listed companies. *Journal of Social and Development Sciences*, 1 (5), 202-207.

Annexes

Annexe 1: Questionnaire n°1

Nom de l'interviewé :.....

Enregistrement n°.....

Guide d'entretien n°1

IDENTIFICATION DE L'INTERVIEWE

Nom :

Age :

Sexe :

Position à l'UCL:

Département :

Ancienneté à l'UCL :

Formation :

Introduction

1. Bonjour, vous serait-il possible de nous faire connaître, de façon succincte, votre parcours professionnel depuis vos études jusqu'à aujourd'hui ?

UCL

2. Combien de personnes travaillent actuellement à l'UCL ?
3. Quelles sont les parties prenantes principales de l'UCL ?
4. Quel est le lien entre les entités dépendantes du CODIR et les autres entités de l'UCL ?
5. Pour qu'un changement dans la méthode de management à l'UCL puisse se faire, quelles sont les formalités à remplir ? Les personnes impliquées dans le processus ?

6. Selon vous, l'UCL doit-elle être gérée comme une grande entreprise ?

La cartographie des détenteurs d'influences

7. Qui sont les groupes d'acteurs impliqués ou les détenteurs d'influence ?
8. Quels sont les enjeux de leur confrontation ?
9. Quels sont les atouts dont chaque groupe dispose ?
10. Quelle stratégie ces différents groupes déploient-ils ?
11. Quelles sont les alliances qui se lient entre les groupes?

Gestion actuelle des risques

12. Quelle est votre définition du risque ?
13. Quels sont les principaux risques identifiés pour l'UCL ? Potentiels ?
14. Certains risques sont-ils actuellement sous-estimés ?
15. Depuis quand le modèle de management du risque a-t-il été mis sur pied ? Est-il remis à jours de temps en temps ? Si oui, à quelle fréquence ? Si non pourquoi ?
16. Pourriez-vous me décrire l'actuel modèle de gestion du risque ?
17. Quels sont les avantages, inconvénients du modèle actuel?
18. Quels sont les différents départements concernés par cette gestion ?
19. Existe-t-il une gestion centralisée des risques ?
20. A qui rapportez-vous les risques identifiés ?
21. Existe-t-il une vérification externe de ses comptes telles celle faite par les big4 pour les grandes entreprises ? Un ICS? Si oui qui s'en charge
22. Est-ce que les fonctions de support comme le Risk Management et l'Audit Interne sont-elles vues comme des coûts à minimiser par l'organisation ?

Projet de changement

23. Quels sont pour vous les objectifs du changement ?
24. Avez-vous déjà parlé en interne d'une sorte de rapport intégré des risques transversaux de l'organisation?
25. Quelles sont les principales barrières à l'implémentation ?
26. Comment pourrait-on atténuer les barrières ?
27. Si elles existent, les barrières peuvent-elles être atténuées ?
28. Voyez-vous plutôt le rapport intégré comme un rapport de coordination des risques ou de centralisation des risques ?
29. Quels seraient selon vous les avantages et inconvénients d'un tel modèle ?
30. Est-ce qu'un tel rapport pourrait aider l'UCL dans la réalisation de ses objectifs ?

Culture de l'UCL

(Voir test OCAI)

Annexe 2: Questionnaire n°2

Nom de l'interviewé :.....

Enregistrement n°.....

Guide d'entretien n°2

IDENTIFICATION DE L'INTERVIEWE

Nom :

Age :

Sexe :

Position à l'UCL :

Département :

Ancienneté à l'UCL :

Formation :

Gestion actuelle des risques

1. Quels sont pour vous le rôle, les missions et la structure organisationnelle d'un département de risk management dans une organisation ? Merci d'étayer votre point de vue.
2. Quels sont pour vous le rôle, les missions et la structure organisationnelle d'un département d'audit dans une organisation ?
3. Actuellement, les risques sont gérés par chaque entité ainsi que par les administrations correspondantes selon le type de risque. Selon le type de risques, la structure s'avère plus ou moins formalisée.
4. Quels sont les avantages et inconvénients de la gestion actuelle des risques ?

5. Certains risques de niveau 1 sont-ils surestimés au niveau de l'université ? En manques-t-ils ?
6. Certains risques sont-ils transversaux ? Sont-ils gérés localement ? Si oui, s'agit-il, pour vous, d'une redondance à travers les différentes entités dans le modèle actuel ?
7. Avez-vous déjà dû faire face à un risque dont vous n'aviez pas la compétence ou la connaissance technique pour le gérer ? Si oui, comment avez-vous réagi ?
8. Selon vous, la structure de l'UCL est-elle principalement centralisée ou décentralisée ?
9. Quels sont les principaux fournisseurs d' « assurance » actuellement à l'UCL ?

Concept « Combined Assurance »

10. Voyez-vous une utilité à ce type de rapport ? Quels est votre opinion sur ce type de rapport ainsi que sur sa nécessité à l'UCL ?
11. Si vous le jugez utile, quelles seraient les barrières à l'implémentation et, le cas échéant, comment les atténuer ?
12. Le modèle des « Combined Assuance » répartit la responsabilité et la gestion du risque de manière structurée sur trois pôles organisationnels : l'entité et l'administration correspondante, le risk management et l'audit : Quels seraient les avantages et inconvénients d'un tel modèle ?
13. Quelles seraient vos attentes d'un tel modèle ?
14. Pensez –vous qu'une telle structure apporterait une valeur ajoutée à l'UCL ? Si oui, laquelle ?
15. Quelles sont les différences entre la gestion des risques au sein d'une entreprise et au sein d'une université ?

Culture au sein de l'UCL

(Voir Test OCAI)

Annexe 3: Questionnaire n°3

Nom de l'interviewé :.....

Enregistrement n°.....

Guide d'entretien n°3 (Audit)

IDENTIFICATION DE L'INTERVIEWE

Nom :

Age :

Sexe :

Position à l'UCL :

Département :

Ancienneté à l'UCL :

Formation :

Gestion actuelle des risques

1. Quels sont pour vous le rôle, les missions et la structure organisationnelle d'un département de risk management dans une organisation ? Merci d'étayer votre point de vue.
2. Quels sont pour vous le rôle, les missions et la structure organisationnelle d'un département d'audit dans une organisation ?
3. Actuellement, les risques sont gérés par chaque entité ainsi que par les administrations correspondantes selon le type de risque. Selon le type de risques, la structure s'avère plus ou moins formalisée.
4. Quels sont les avantages et inconvénients de la gestion actuelle des risques ?

5. Certains risques de niveau 1 sont-ils surestimés au niveau de l'université ? En manques-t-ils ?
6. Certains risques sont-ils transversaux ? Sont-ils gérés localement ? Si oui, s'agit-il, pour vous, d'une redondance à travers les différentes entités dans le modèle actuel ?
7. Avez-vous déjà dû faire face à un risque dont vous n'aviez pas la compétence ou la connaissance technique pour le gérer ? Si oui, comment avez-vous réagi ?
8. Selon vous, la structure de l'UCL est-elle principalement centralisée ou décentralisée ?
9. Quels sont les principaux fournisseurs d' « assurance » actuellement à l'UCL ?

Audit

10. Quelle est la mission actuelle du service d'audit et sa structure ?
11. L'UCL utilise-t-elle les standards internationaux tels que prescrits par l'IIA ?
12. Quelle méthodologie utilisez-vous pour vos rapports d'audit ?
13. A quelle fréquence mettez-vous à jour votre plan d'audit interne ?
14. En cas de recours à l'audit externe, pensez-vous que la mise en place d'un modèle de « Combined Assurance » ou de gestion de risque réduira-t-il les « external audit fees » ?
15. Quelle est votre perception de l'audit externe ?

Concept « Combined Assurance »

16. Voyez-vous une utilité à ce type de rapport ? Quels est votre opinion sur ce type de rapport ainsi que sur sa nécessité à l'UCL ?
17. Si vous le jugez utile, quelles seraient les barrières à l'implémentation et, le cas échéant, comment les atténuer ?
18. Le modèle des « Combined Assuance » répartit la responsabilité et la gestion du risque de manière structurée sur trois pôles organisationnels : l'entité et l'administration correspondante, le risk management et l'audit : Quels seraient les avantages et inconvénients d'un tel modèle ?
19. Quelles seraient vos attentes d'un tel modèle ?

20. Pensez –vous qu'une telle structure apporterait une valeur ajoutée à l'UCL ? Si oui, laquelle ?
21. Quelles sont les différences entre la gestion des risques au sein d'une entreprise et au sein d'une université ?

Culture au sein de l'UCL

(Voir Test OCAI)

Annexe 4: Test OCAI

Test OCAI (Organizational Culture Assessment Instrument)

Nom du participant :.....

		Situation actuelle	Situation idéale
1. Caractéristiques dominantes	A. L'organisation est un endroit très spécial. C'est comme une famille élargie. Les gens semblent y partager beaucoup d'eux-mêmes.		
	B. L'organisation est un endroit très dynamique et à l'esprit entrepreneurial. Les gens sont prêts à se mouiller et à prendre des risques.		
	C. L'organisation est très orientée vers la production. Une préoccupation majeure est de faire le travail. Les gens sont très compétitifs et axés sur la réussite.		
	D. L'organisation est un endroit formalisé et structuré. Les procédures bureaucratiques sont très présentes et régissent ce que les gens font.		
2. Les leaders de l'organisation	A. Les dirigeants de l'organisation sont généralement considérés comme des mentors, des modérateurs, voire des figures parentales.		
	B. Les dirigeants de l'organisation sont généralement considérés comme des entrepreneurs, des innovateurs ou des preneurs de risques.		
	C. Les dirigeants de l'organisation sont généralement considérés comme des producteurs, des compétiteurs, obsédés par la performance.		
	D. Les dirigeants de l'organisation sont généralement considérés comme des coordinateurs, organisateurs, des spécialistes de l'efficacité		

3. Gestion des employés	A. Le style de gestion se caractérise par le travail en équipe, le consensus et la participation.		
	B. Le style de gestion de l'organisation est caractérisé par la prise de risque individuelle, l'innovation, la flexibilité et l'unicité.		
	C. Le style de gestion de l'organisation est caractérisé par une forte motivation à la compétition, la mise en place et l'atteinte de forts objectifs		
	D. Le style de gestion de l'organisation se caractérise par une surveillance attentive de la performance, la volonté de tout prévoir et planifier.		
4. La colle de l'organisation	A. La colle qui tient l'ensemble de l'organisation est la loyauté et la confiance mutuelle. L'engagement envers l'organisation est élevé.		
	B. La colle qui tient l'ensemble de l'organisation est l'orientation vers l'innovation et le développement. Il y a une volonté d'être à la pointe de ce qui se fait, être les plus brillants.		
	C. La colle qui tient l'ensemble de l'organisation est l'accent mis sur la production et l'atteinte des objectifs. L'agressivité est un thème commun.		
	D. La colle qui tient l'ensemble de l'organisation est la présence de règles formelles et politiques. Le maintien du bon fonctionnement de l'organisation est très important.		
5. Levier stratégique	A. L'organisation met l'accent sur le développement humain, la confiance mutuelle, l'ouverture et la participation.		
	B. L'organisation met l'accent sur l'acquisition de nouvelles ressources et l'atteinte de nouveaux défis. Essayer de		

	nouvelles choses et prospecter de nouvelles opportunités sont des éléments mis en valeur.		
	C. L'organisation met l'accent sur les actions concurrentielles et l'atteinte d'objectifs. La mesure des objectifs est dominante.		
	D. L'organisation met l'accent sur la permanence et la stabilité. L'efficacité et le bon fonctionnement de l'organisation au quotidien sont des éléments importants.		
6. Critères de succès	A. L'organisation définit le succès sur la base du développement des ressources humaines, du travail en équipe et d'une réelle considération pour les personnes.		
	B. L'organisation est définie sur base du développement des produits/services les plus récents et les plus uniques qui soient sur le marché ; être les leaders du marché en termes d'innovation.		
	C. L'organisation définit le succès sur la base de la pénétration du marché et du nombre de parts de marché. Être le leader sur le marché concurrentiel est un élément clé.		
	D. L'organisation définit le succès sur la base de l'efficacité : planification, livraisons fiables, production à faibles coûts sont des éléments du succès.		

Annexe 5: Interview n°1

Résumé - Interview #1	
Nom : [redacted]	**Date :** 12 février 2015
Fonction : [redacted]	**Time :** 33 min
Guide: N°1	**Contact :** interview semi-structured

UCL

Actuellement, plus ou moins 5000 personnes travaillent pour l'UCL (hors hôpitaux et académiques extraordinaires).

Le projet d'implémentation est à destination du CODIR. Le CODIR est un rassemblement des directeurs des principales administrations, des services en staff de l'administration (comme l'audit ou le service de radioprotection) et les directeurs de DAF. C'est une entité de discussion et de consultation.

L'UCL est gérée dans une certaine mesure comme une entreprise publique de manière bicéphale dans sa partie administrative, moins dans la partie académique. Même si c'est une université de droit privé, l'UCL opère dans une sphère publique.

LA CARTOGRAPHIE DES DETENTEURS D'INFLUENCE

Pour réussir le projet, il faut s'intéressé aux acteurs qui peuvent mettre sur pied le projet. Il s'agit des membres du CODIR mais également le monde académique via les présidents d'institut et doyens de faculté.

Chaque groupe dispose de plusieurs atouts. L'académique a une vision sur ses objectifs de recherche en donnant la voie qu'il veut suivre. L'administratif se met au service des objectifs de l'académique. L'administratif est à même de gérer les différentes contraintes qui se présentent à l'UCL, notamment les contraintes juridiques qui sont nombreuses.

Il existe des alliances et des mésententes entre les deux groupes. Historiquement il y a une certaine séparation mais sur le terrain ça se passe plutôt bien. Il faut parfois répéter à l'académique les contraintes et à l'administratif l'objectif d'enseignement et de recherche. Un certain équilibre existe.

GESTION ACTUELLE DU RISQUE

A l'UCL, les principaux risques sont le risque informatique (reprenant la gestion des étudiants, et la gestion financière), le risque étudiant et le risque de GRH.

L'étude exploratoire a laissé une certaine liberté aux interviewés quant à leur réponse. Il se peut que certains risques importants pour l'institution aient été éludés. Certains risques sont donc sous-estimés et d'autre surestimés. Il appartient au « risk manager » de débroussailler tout ça.

Actuellement aucun modèle de « risk management » n'existe si ce n'est que chaque personne gère son risque en interne en bon père de famille. Cette gestion n'est ni formalisée ni centralisée.

De ce qu'il ressort des interviews de l'étude exploratoire, il faudrait mettre sur pied un « risk management » sans que ce département ne coûte trop cher. L'idée est en général bien reçue pour l'établissement de ce dernier. L'audit est un outil légal et donc est accepté comme tel.

PROJET DE CHANGEMENT

Les objectifs de ce projet étaient à la base l'optimalisation des contrats d'assurance. Sans connaissance des risques existants, on ne peut pas s'assurer de manière optimale. Cette situation a quand même évolué dans le bon sens depuis quelque temps, on peut citer pour exemple le plan interne d'urgence.

Le manque de centralisation de la gestion des risques est un facteur de risques. Par rapport aux contrats d'assurance, il y a des contrats parapluies qui ne sont pas précis et mal adaptés pour l'UCL.

Le risk management devrait être là pour coordonner les générateurs de risques et les coordinateurs de risques. Certains risques pouvant être multidimensionnels, il pourra y avoir plusieurs coordinateurs de risques. Il doit « lier la sauce ». La question est de voir jusqu'où on peut aller.

Certaines barrières pourront apparaître : l'aspect de coût, l'aspect culturel et l'aspect psychologique (peur de se faire déposséder).

Annexe 6: Interview n°2

Résumé - Interview #2	
Nom : [redacted]	**Date :** 16 mars 2015
Fonction : [redacted]	**Time :** 54 min
Guide: N°2	**Contact :** interview semi-structured

GESTION ACTUELLE DES RISQUES

L'UCL possède une structure spécialisée pour l'administration centrale. Les facultés jouissent d'une assez grande liberté tant qu'elles restent dans les enveloppes fermées qui leur sont dédiées (une pour le personnel et l'autre pour le budget).

Actuellement, chaque risque est géré de façon locale, c'est à dire que chaque directeur est amené à gérer son risque de façon autonome. L'avantage de cette méthode est que le directeur est le plus à même de connaître/identifier ses propres risques mais, par la force de l'habitude on risque de ne plus les voir. Pour améliorer le processus, il faut pouvoir consolider les différents risques et aider les acteurs à les identifier (ex : questionnaires, interview, …). Une structure extérieure aux départements peut donc être utile à cette identification.

Par rapport aux risques de niveau 1 qui ont été identifiés lors de l'étude exploratoire, les risques ont été bien estimés mais il faudrait rajouter le risque du changement politique (cf. Décret Marcourt). On peut citer comme exemple le changement occasionné dans les frais d'inscription et la suppression des frais supplémentaires de seconde session occasionnant un manque à gagner pour l'UCL qui doit revoir certaines de ses dépenses à la baisse.

Certains risques transversaux existent. On citera principalement le risque informatique dû à la centralisation de ce dernier. Des difficultés récurrentes existent surtout avec l'implémentation du programme SAP qui ralentit le travail de certaines administrations (dont celle de l'ADAE). La situation financière est également un risque transversal pour

l'université. En effet, le financement par étudiants diminue d'année en année.

Par rapport à la redondance de la gestion des risques, il faudrait que ceux-ci soient mieux arbitrés et harmonisés. Il faudrait les centraliser et réaliser un arbitrage des risques par la suite.

Dans la situation actuelle, si une administration fait face à un risque pour lequel elle n'a pas la capacité technique ou la connaissance nécessaire pour pouvoir le gérer elle peut aller chercher de l'aide dans un autre département. Cette demande d'aide n'est actuellement pas formalisée et/ou obligatoire. Il y a le dnager de ne pas se faire aider par la personne la plus à même de gérer ce risque. Aucune liste de compétences n'existe sauf pour les départements légaux.

Les principaux fournisseurs de sûretés proviennent principalement de l'administration financière (fournissant des balises), de l'audit externe (Ernst&Young) et de l'audit interne. L'auditeur interne conserve son indépendance, ce dernier rapportant uniquement au comité d'audit. Il n'est pas vu comme uniquement un contrôleur parce qu'il fournit des conseils aux différentes entités qu'il audite.

IMPLEMETATION D'UN ERM ET « COMBINED ASSURANCE »

Mettre sur pied un ERM permet de façon plus globale d'identifier les risques et de montrer aux autorités (conseil rectoral) les difficultés/priorités des départements. Ça permet également de mettre en évidence certains risques pouvant aider le management dans la prise de décision dans des domaines où il ne sait pas assumer de manière optimale ses responsabilités. L'UCL a une fâcheuse tendance à rajouter des éléments sans forcément en supprimer d'autres, et à aller au-delà des capacités des administrations (en termes de ressources financière, humaines, …).

Certaines barrières peuvent apparaître pour l'implémentation d'un ERM. Tout d'abord, certaines administrations ne sont pas favorables au rajout de balises/contrôles de leur travail. De plus, il y a une augmentation de l'esprit de compétition au sein de l'UCL (surtout au cours des 10 dernières années).

Il appartient au top management de l'université de donner une priorité à l'implémentation si elle estime qu'il est important de le faire.

Actuellement il n'y a pas d'obligation d'instaurer un ERM, il ne deviendra peut-être jamais une obligation mais c'est assez important à partir du moment où on dépasse une certaine taille. Il peut y avoir un risque à rendre obligatoire l'implémentation des ERM si les acteurs, une fois celui-ci rendu obligatoire, tentent tout pour contourner cette obligation. La mise en place d'un ERM apporterait néanmoins une valeur ajoutée à l'UCL

Les risques entre le monde de l'entreprise et celui des universités peuvent être fortement différent (ex : risque sur une chaîne de montage) mais pour certains ils peuvent être assez semblables (ex : risque financier).

CULTURE DE L'UCL

La culture de l'UCL a fortement changé depuis les 10 dernières années. On a perdu la « patte UCL » avec beaucoup de recrutements de personnes provenant de l'extérieur. Dans le passé les gens faisaient toute leur carrière à l'UCL. Cet apport à l'avantage d'avoir une vision venant de l'extérieur mais l'inconvénient d'une perte de culture d'entreprise.

Pour les décisions externes, ces dernières s'imposent. Pour les décisions internes, c'est un peu comme faire manœuvrer un paquebot. S'il faut changer de cap, c'est assez compliqué.

Il y a une certaine résistance au changement qui est favorisée par la culture de l'université. Pour réussir un changement, il faut donc pouvoir fournir aux différentes administrations une bonne information de manière assez simple.

Annexe 7: Interview n°3

Résumé - Interview #3	
Nom : [redacted]	**Date :** 17 mars 2015
Fonction : [redacted]	**Time :** 60 min
Guide: N°2	**Contact :** interview semi-structured

GESTION ACTUELLE DES RISQUES

Il y a de nombreux risques à l'UCL. Le principal tourne autour de la réputation de l'institution.

Actuellement aucune gestion du risque n'est mise sur pied à l'UCL. Deux départements sont appelés à entrer dans le processus, celui de « risk management » et le département d'audit. Les missions du département de « risk management » permettent de mettre en évidence les risques que les entités subissent d'une part et qu'elles créent d'autre part. Cela amène une culture de la gestion du risque présent. Il appartient également au département de quantifier le risque. Le « risk manager » doit mettre sur pied une formation pour que tous les acteurs puissent être initiés à cette gestion.

Actuellement, on parle principalement d'audit financier et organisationnel à l'UCL. L'audit organisationnel est un outil important dans la gestion du risque mettant en évidence les failles dans l'organisation.

L'auditeur de l'UCL possède une indépendance légale avérée dans les faits.
Dans le système actuel, les risques sont gérés par chaque entité, il faut que le producteur du risque reste impliqué dans le processus mais il faut que cette gestion soit encadrée par le « risk manager ».

Dans le travail préparatoire de Marc Rombouts sur les risques présents dans les entités du CODIR, une cartographie des risques a été réalisée. On ne peut pas dire si les risques ont été quantifiés de manière optimale mais il est important de les prendre néanmoins en compte. Certains risques sont transversaux. Actuellement, le risque informatique dû à la centralisation de ce dernier est géré de manière centralisée. L'expérience montre qu'il manque un « Monsieur Qualité » pour vérifier la qualité et la pertinence de l'information (l'UCL n'ayant mis sur pied qu'un « Monsieur Sécurité »).

Il peut arriver que certains acteurs n'aient pas la compétence technique pour gérer le risque. Il vaut mieux se faire aider par une personne compétente plutôt que d'essayer de gérer le risque soi-même, ce qui aggraverait la situation. Il ne serait pas inutile de créer une liste de personnes de référence. Il est à noter que cette liste est d'une importance capitale pour les départements AUST/SVUC/SET.

La structure de l'UCL est assez hybride. Il y a une administration centrale mais le reste de l'université est très décentralisé (par exemple les instituts de recherches qui sont très indépendants). Si on comparait l'université à une entreprise, les facultés pourraient être assimilées à des filiales jouissant d'une grande indépendance mais restant dépendantes financièrement de l'université. Les instituts de recherches, eux, possèdent une plus large autonomie et doivent chercher leurs financements par eux-mêmes.

Les principaux fournisseurs de sûretés de l'UCL sont le « groupe des juristes », service d'étude (dans sa dimension juridique) et l'audit interne. Il aurait été intéressant de rajouter les responsables de projet IT, par une gestion en aval plus importante. Malheureusement, ça ne s'est jamais réalisé.

IMPLEMETATION D'UN ERM ET « COMBINED ASSURANCE »

La cartographie des risques est utile pour une bonne administration de l'université, il peut permettre d'en supprimer certains bien que ça ne soit pas son principal but (qui est l'identification).

L'outil présenté de manière brut est très anglo-saxon. C'est un processus qui crée une charge de travail supplémentaire pour certains acteurs ne bénéficiant pas forcément de l'outil. Il est très important de rester simple et peu invasif. Cette complexification serait une des plus grandes barrières à l'entré. Il faut éviter la lourdeur inutile pour le chic de la chose.

Il faut également faire attention de ne pas déresponsabilisé les acteurs par l'implémentation. Il faut, pour éviter ces dérives impliquer les différentes parties prenantes.

Pour certains risques, comme les déchets radioactifs, une gestion par d'autres personnes peut apporter au contraire un plus grand confort pour l'UCL.

Une amélioration de la gestion des risques apportera surement une valeur ajoutée à l'UCL. Il faut, néanmoins ne pas investir plus que nécessaire. En restant dans une sage proportion, le

coût ne devrait pas être trop important tout en restant efficace.

Il faut que tout le monde puisse avoir de manière intuitive une bonne compréhension de la gestion des risques et de ses avantages.

La gestion des risques dans une université et dans une entreprise est assez semblable bien que l'objectif poursuivi ne soit pas le même.

CULTURE DE L'UCL

Les principaux changements que subit l'UCL viennent principalement de l'externe (et principalement de la Fédération Wallonie-Bruxelles). Il y a une certaine lassitude des changements venant aussi bien de l'interne et de l'externe. Il appartient aux autorités de l'UCL d'essayer de minimiser les problèmes liés aux changements pour épargner les différents acteurs de terrains.

Annexe 8: Interview n°4

Résumé - Interview #4	
Nom : [redacted]	**Date :** 18 mars 2015
Fonction : [redacted]	**Time :** 34 min
Guide: N°2	**Contact :** interview semi-structured

GESTION ACTUELLE DES RISQUES

Actuellement, il n'y a pas de gestion formelle des risques à l'UCL. Le rôle du « risk manager » est d'identifier, de couvrir et d'assurer les différents risques auxquels une organisation doit faire face. Il doit assurer ces risques pour éviter qu'il n'y ait une perturbation dans la société. Sa mission est à la fois tournée vers l'intérieur et sur l'extérieur à la différence de l'audit interne qui est centré sur l'intérieur.

L'auditeur interne doit vérifier l'existence des procédures et le respect de celle-ci par les différents départements. Il ne va pas jusqu'à l'identification des risques. L'audit interne est beaucoup plus restrictif que le risk management.

Ce sont deux fonctions complémentaires, le risk manager doit s'appuyer sur le travail de l'auditeur et franchir une étape supplémentaire.

L'auditeur conserve son indépendance, relevant directement du comité d'audit.
Dans la gestion actuelle, le directeur ne perçoit pas toujours le risque vu que ce dernier fait partie du quotidien et il manque donc d'anticipation. Il faut néanmoins conserver l'implication du directeur dans le processus pour qu'il soit optimal.

Le risk mapping est une étape importante qui mérite attention. En effet, les risques sont souvent sous-estimés vu qu'ils appartiennent au quotidien des directeurs d'administration. De nombreux risques sont transversaux, ils sont assez difficiles à gérer car personne ne se les

approprie et ils peuvent faire l'objet de duplication. Une fonction centralisée du risque permettrait d'éviter ce genre de désagrément.

Si on manque de capacité technique pour gérer un risque, on peut passer à côté du risque sans s'en apercevoir.

La structure de l'UCL est généralement décentralisée et donc la gestion des risques devient en quelque sorte nécessaire pour manager au mieux l'UCL.
Pour être efficace, dans le processus de gestion des risques, il faut intégrer les structures périphériques qui sont aussi génératrices de risques.

Les fournisseurs de sûreté de l'UCL sont l'audit interne, l'audit externe (E&Y), les délégués du gouvernement, la Cour des Comptes, les différents comités qui sont là pour donner des guidelines (comité d'audit, conseil académique, comité de gestion des ressources extérieures,…). Ces organes sont là pour identifier l'ensemble des problèmes.
L'UCL dont la mission principale se trouve dans l'enseignement et la recherche se doit donc, avec les moyens qui lui sont alloués, de maximiser les fonctions d'enseignement et de recherche.

Gaspiller les moyens budgétaires à des dépenses inutiles et perdre l'octroi de subsides constituent les risques les plus graves.

IMPLEMETATION D'UN ERM ET « COMBINED ASSURANCE »

Une gestion des risques permet de mieux les suivre et de mieux les identifier. Ce qui permet de mieux les gérer in fine.

Actuellement, il n'y a pas de risk management en Europe Continentale, l'implémenter est une attitude proactive de l'UCL. A terme, on sera presque obligé de le faire. Un peu comme le comité d'audit qui n'était pas une obligation mais qui est quasi obligatoire aujourd'hui.
Il faut veiller à ce que cette fonction soit de la même ligne hiérarchique que le département d'audit interne. Il faut veiller à lui confier une certaine indépendance.

Il faut donc être vigilant afin que le système ne soit pas trop contraignant pour l'ensemble des administrations et leur laisser une marge de manœuvre.

La répartition sur les trois lignes de défenses du management permet de s'assurer qu'on couvre l'ensemble des risques auxquels l'UCL est confrontée, d'avoir des visions différentes et complémentaires. Il faut faire attention que ce système ne soit trop contraignant pour l'ensemble des administrations, enlevant les initiatives aux départements. Il faut laisser une marge de manœuvre aux administrations.

En tant que directeur financier, le modèle devrait permettre de mieux conscientiser les différentes administrations de l'UCL aux risques. Un peu comme le département d'audit de l'UCL qui est là pour accompagner, aider à identifier les problèmes et améliorer les processus.

Ce projet apportera une valeur ajoutée à l'UCL en évitant une déperdition des moyens budgétaires.

Il n'y a pas de différences entre la gestion des risques à l'UCL et dans une entreprise. La finalité est différente mais pas la gestion des risques.

CULTURE DE L'UCL

Les grands changements que subit l'UCL sont consommateurs de temps mais ils donnent la possibilité de se remettre en question. Les changements évitent d'entrer dans une certaine routine. Un peu comme dans la gestion du risque, sans se remettre en question, on entre dans une certaine myopie par rapport aux risques.

Annexe 9: Interview n°5

Résumé - Interview #5	
Nom : [redacted]	**Date :** 17 avril 2015
Fonction : [redacted]	**Time :** 60 min
Guide : N°2	**Contact :** interview semi-structured

GESTION ACTUELLE DES RISQUES

Actuellement, il n'existe pas de gestion des risques globalisée. Le département de sécurité et de radioprotection est assez particulier car ce dernier doit gérer ses risques en interne (en tout cas pour les risques directement liés aux départements).

Le département de risk management doit apporter une aide et un support aux différentes activités que nous gérons. Il doit également aider à la réalisation des contrats pour être sûr qu'aucun problème ne puisse survenir par la suite. C'est une nécessité pour le bon fonctionnement de l'UCL, y compris dans ses relations avec les tiers.

Il n'y a pas d'attente particulière de la part du département d'audit interne pour le département du fait de l'importance des contrôles externes qui sont réalisés par les différents organismes externes de l'UCL. Le département est reconnu expert par arrêté ministériel et il est logique que la mise en œuvre émane du département.

Dans la gestion des risques actuels, certains sont transversaux dans leur gestion, pas forcément dans l'objet de ceux-ci. Certains risques, comme la gestion des plans d'urgence, sont dans leur nature transversale à l'ensemble de l'UCL. Il faut essayer de les coordonner.

Lorsqu'un risque survient, risque dont le département ne détient pas la capacité technique pour la gestion de ce dernier, si la compétence n'existe pas en interne à l'UCL, il fait appel à

des bureaux externes. Dans certains cas, bien que la compétence existe à l'UCL, pour éviter d'être contrôleur-contrôlé, le département « outsource » le problème à un bureau externe. Il n'existe pas de liste de compétence au sein de l'UCL, on est plus guidé par leur réputation. L'établissement d'une liste faciliterait le travail.

Utiliser certaines ressources humaines présentes à l'UCL comme les professeurs des différentes facultés serait également à conseiller. Ce qui n'est pas le cas dans la situation actuelle.

La structure de l'UCL est très décentralisée, ressemblant au système féodal en tout cas dans la partie enseignement et recherche. « Chacun est chef dans sa tour ». Il n'y a pas de relation entre les différentes entités du site, ce qui crée une concurrence entre entités et une duplication de certains outils.

L'administration fonctionne exactement comme celle d'une entreprise, la partie administrative

IMPLEMETATION D'UN ERM ET « COMBINED ASSURANCE »

Toutes atteintes à l'image entrainent des conséquences désastreuses pour l'UCL. En effet, cette atteinte à l'image pourrait diminuer le nombre d'étudiants et/ou de chercheurs et donc diminuer le financement de l'UCL. La gestion des risques doit éviter par anticipation que les risques puissent atteindre l'image de l'UCL. On ne sait pas jouer directement sur l'image mais sur tous les facteurs qui l'impacteront.

La gestion du risque est équivalente dans la gestion des risques par rapport à la gestion faite dans une entreprise.

La cartographie des risques est un bon outil pour donner des priorités à la gestion des risques. Cet outil est utile pour la gestion de l'UCL.

L'implémentation d'un ERM est une nécessité si on veut donner les moyens à la mise en

œuvre. Il faut une bonne utilisation du processus pour mieux gérer l'UCL. L'ERM apporte une certaine connaissance de l'entité aux différents acteurs.

L'implémentation est un outil qui devrait permettre à l'UCL de rester concurrentielle afin d'améliorer son image de marque de l'université. Il faut donc assurer que la moindre crise ne vienne pas casser le développement de l'UCL.

Des barrières dans l'implémentation peuvent apparaitre, principalement de fait qu'il s'agit d'un changement. Un nouveau processus peut donner l'impression de rajouter une lourdeur administrative supplémentaire et donc mal passer auprès des entités de l'UCL.

La gestion par les trois lignes de défenses du management permet de prendre un certain recul par rapport aux risques et d'éviter une certaine myopie en occultation des risques. Il faut une vue au jour-le-jour mais également une analyse à long terme sur la gestion.

Les fournisseurs de sûreté sont multiples pour l'UCL. Le département en est un également un pour les risques qu'il doit gérer. Le département doit assurer l'administrateur général que les procédures sont bien suivies. On peut citer, de manière plus globale, il y a également l'audit, le service juridique et E&Y.

L'implémentation d'un processus de risque management apporterait une valeur ajoutée à l'UCL et améliorerait la gestion des risques par une uniformisation et une coordination de la gestion. Il faut surtout éviter de se renvoyer les risques entre départements pouvant aboutir à une non-gestion de l'un ou l'autre de ceux-ci. Un département n'est pas à même de gérer tous les risques qu'il produit.

CULTURE DE L'UCL

Le département n'est pas fortement impacté par les gros changements organisationnels mais il est de plus en plus sollicité pour les problèmes liés à la sécurité. On a amélioré les processus pour les départements. On sent qu'on va vers une processus de gestion du risque.

Annexe 10: Interview n°6

Résumé - Interview #2	
Nom : [redacted]	**Date :** 16 mars 2015
Fonction : [redacted]	**Time :** 48 min
Guide : N°3	**Contact :** interview semi-structured

GESTION ACTUELLE DES RISQUES

Actuellement il n'y a pas de gestion des risques de manière formelle à l'UCL. Le département de « risk manager » a pour but de mettre en évidence les différents risques présents dans les organisations. Cette identification commence par la cartographie des risques. Il pourrait être intéressant de rajouter un élément non encore présent dans la est cartographie issue de l'étude exploratoire, à savoir la vélocité du risque.

La gestion actuelle des risques ne permet pas de faire circuler l'information. Il manque donc l'étape de validation. Il peut y avoir également une erreur d'approximation de la part des directeurs. La cartographie est la première étape devant être suivie par celle de la validation.

Certains risques sont transversaux, on peut citer pour exemple le risque de réputation, le risque informatique, la perte d'un contrat. Ils sont néanmoins gérés localement, il y a donc une redondance dans la gestion du risque. Toutefois une redondance de l'identification ou de suivi peut être positive. Dans le cas de la redondance la pire des solutions est la non-gestion du risque en croyant qu'une autre personne la gère.

Il faut donc une sorte de champion du risque qui coordonne les différentes actions pour être certain que le risque soit géré de la manière la plus optimale. Il faut connaître les limites de ses compétences et ne pas les outrepasser.
L'UCL possède à la fois une structure centralisée et décentralisée. Une partie est

décentralisée par l'existence des instituts et facultés et par l'existence des secteurs tout en restant centralisée sur d'autres éléments comme par l'existence de l'administration.

Les principaux fournisseurs de sûreté sont E&Y, l'audit et le département des risques et patrimoines. On peut également intégrer les fournisseurs externes comme la Cour des Comptes, les commissaires du gouvernement,… Le département légal participe aussi au processus de sûreté.

AUDIT

La mission actuelle du service d'audit se situe à quatre niveaux. Premièrement la réalisation d'audit tel que défini par le comité d'audit, deuxièmement, le contrôle des ASBL périphériques, troisièmement le contrôle des sociétés qui désirent s'implémenter dans le parc scientifique et finalement de façon plus marginale des audits de fraudes, des avis techniques demandés au niveau du service.

Le comité d'audit est une émanation du CA. Il est présidé par le président du Conseil d'Administration et il y a un certain nombre d'administrateurs qui ne sont pas forcément de l'UCL.

On attend de l'auditeur à l'UCL qu'il donne la température sur les procédés et donne son approbation ou sa désapprobation. L'audit se base sur les standards de l'IIA.

La méthodologie utilisée pour les rapports d'audit tend vers la simplicité. La structure du rapport suit un scope bien défini et on essaye de ne pas outrepasser le scope défini. On tente de repérer les risques et on formule des recommandations. Cette méthode tranche avec l'ancienne méthode d'audit de l'UCL en évitant les rapports lyriques. Ils sont principalement basés sur la sauvegarde du patrimoine, la légalité, la fiabilité etc. Le tout avec un souci de fluidité et de transparence. Cette méthode permet de pointer les inefficacités.

Chaque année une réunion annuelle définit le plan d'audit qui va être réalisé.

IMPLEMETATION D'UN ERM ET « COMBINED ASSURANCE »

L'implémentation d'un ERM est primordiale pour l'université. C'est un élément essentiel pour obtenir le meilleur fonctionnement possible de l'institution. L'implémentation est proactive et apportera une grande valeur ajoutée à l'UCL. Cette valeur ajoutée est la cohérence et la non duplication de la gestion des risques.

Certaines barrières risquent néanmoins d'apparaître mais seulement à un niveau ou les gens sont assez intelligents et compétents pour que, après un temps d'adaptation, le côté positif prenne le dessus

L'implémentation du modèle d'un ERM ne réduira en rien les « external audit fees » en tout cas d'après E&Y.

Il n'y a aucun désavantage à coordonner les risques vu que tout le monde poursuit les mêmes objectifs généraux.

Bien que l'objectif final ne soit pas le même que dans le monde de l'entreprise, les risques doivent être gérés de la même manière.

CULTURE DE L'UCL

Les changements d'ordre politique, s'ils ne sont pas bien compris, ne sont pas acceptés. La résistance au changement est assez grande du fait du processus démocratique.

Annexe 11: Exemple des politiques et procédures ERM de l'Université d'Aberdeen

UNIVERSITY OF ABERDEEN

RISK MANAGEMENT POLICY & PROCEDURES

1 INTRODUCTION

This document sets out the policy and procedures for risk management within the University and replaces earlier documentation.

The risk management process is formally integrated with the University's strategic planning process and the monitoring of performance against objectives. There is also a close interface between the University's risk management and audit functions. The University Audit Committee requires to be satisfied as to the effectiveness of the mechanisms operated by the University for identifying, assessing and managing risks and states its opinion in the Audit Committee Annual Report to the University Court and the Scottish Funding Council.

The University Register of Strategic (or Corporate) Risks directly correlates with the University's strategic aims and institutional Key Performance Indicators within the Strategic Plan (2011 - 2015). The register is an electronic document to which appropriate staff have read-only access, with designated "Risk Champions" in each area of activity having responsibility for notifying updates to the Risk Co-ordinator within Policy, Planning and Governance.

The Register of Strategic Risks will be updated in conjunction with the development of the Strategic Plan, ensuring continuing consistency between strategic objectives and strategic risks.

The risk management model has been extended to, and adopted at College and Directorate levels. This embeds risk management across all activities and provides a visible and Integrated Risk Management (IRM) system whereby local risk registers inform the institution-wide risk management process and Register, and *vice versa.* Heads of College and Directors are responsible for managing the roll out of the IRM model at Schools and administrative section levels, with appropriate local re-calibration of Likelihood and Impact scoring.

The process has been rolled out to all University Projects. Project Boards are responsible for the monitoring of Project Risks with onward reporting via the Capital Programme Monitoring Group to the University Management Group.

Risk is a standing item in Committee papers and discussed in all University Committees and Advisory Groups.

2 WHY RISK MANAGEMENT?

We manage our Risks in order to ensure that we achieve our objectives.

The benefits of undertaking Risk Management include:

- Making achievement of objectives more likely
- Making damaging events less likely
- Reducing the time spent on "fire-fighting"
- Leading to a more efficient use of capital and resources
- Improving the quality of service
- Supporting better planning
- Enabling a more effective exploitation of opportunities
- Promoting collaborative working
- Informing decision-making
- Providing assurance to stakeholders
- Protecting the University's reputation
- Facilitating improved performance

Risk management is not a bureaucratic form-filling exercise, it is a way to organise and record our thoughts, integrating risk assessment and planning into all of our activities.

3 DEFINITIONS

3.1 RISK

The HM Treasury "Orange Book" which is regarded as the "standard text" for Public Sector Risk Management practice, defines a risk as being:

"Any uncertainty of outcome, positive opportunity or negative threat, of actions and events in the delivery of objectives." (HM Treasury: Assurance, 2004)

It is important to recognise the difference between a risk and an issue.

- If something has an uncertain outcome, it is a Risk
- If there is no uncertainty, it is an Issue

Examples of Issues, which the University manages through its normal working practices include; compliance with the terms of software licensing arrangements; budgetary control; and implementation of Research Council governance and ethics requirements. Where a perceived Risk is avoidable through good management it is likely that the risk is a mitigating factor rather a risk in itself. E.g. "poor project management" - here the mitigating action is robust project management.

Note: 7/11/14 Forthcoming Project Management Methodology proposes that if a risk becomes an issue – in other words the risk has become reality – it should be marked as an issue and added to the issue log. Further information will follow.

The University Register of Strategic Risks will contain only Risk items, of an agreed financial value or correspondingly severe level of impact, as defined at 3.4 and 3.5 below, which impact upon institutional objectives. These objectives are as stated in the current Strategic Plan.

At College/Directorate level, Risk Registers will contain only Risks to the achievement of College/Directorate objectives as stated in Operational Plans. Such plans will interface with the University's Strategic Plan through operationalisation of the University's strategic objectives.

3.2 UNIQUE RISK REFERENCES

Each Risk will be allocated a unique reference number, which it will retain in perpetuity, and will appear in a single SORF category as described below *(3.6).*

3.3 THE IDENTIFICATION AND STATEMENT OF RISKS

It is the responsibility of all members of staff to identify risks to the University achieving its objectives, and to notify them to the Risk Champion in their area. (*See 4, Roles and Responsibilities)*

The title of a Risk appearing on the Risk Register should be concise but contain sufficient information to distinguish it from the others.

The description of a risk *(documented within a Risk Action Plan, see Templates and 3.8 below)* should include some background on its causes and impact upon objectives.

The following simple example is taken from the "Orange Book":

Objective – to travel from A to B for a meeting at a certain time	
Failure to get from A to B on time for the meeting	This is not a risk, this is simply the converse of the objective
Being late and missing the meeting	This is a statement of the impact of the risk, not the risk itself
There is no buffet on the train so I get hungry	This does not impact on achievement of the objective
Missing the train causes me to be late and miss the meeting	This is a risk which can be controlled by making sure I allow plenty of time to get to the station
Severe weather prevents the train from running and me from getting to the meeting	This is a risk which I cannot control, but against which I can make a contingency plan

3.4 THE UNIVERSITY'S RISK APPETITE

Risk Management requires the defining of an organisation's Risk Appetite. This means;

"the extent to which the University is tolerant of or averse to Risk."

The University Court reviews the University's overall Risk Appetite each year. This is currently defined as being "not beyond Major" (Impact) and with corresponding Likelihood graded at 4 or above in the scale noted at 3.5 below.

Such Risks will appear in the Red/Amber shaded areas of the Risk Map (see 3.7 below).

3.5 LIKELIHOOD AND IMPACT

Risks require to be scored to reflect the **Likelihood** of their occurring and their **Impact** if they were to occur. The basis of University-level scoring is as follows:

Likelihood is to be graded at 6 levels:

>1 in 10	Is expected to occur in most circumstances	6
1 in 11 – 100	Will probably occur	5
1 in 101 – 1000	Could occur at some time in the future	4
1 in 1001 - 10,000	Might occur, but doubtful	3
1 in 10,001 - 100,000	May occur, but only in exceptional circumstances	2
<1 in 100,001	Extremely unlikely to occur	1

Impact is to be graded at 6 levels:

Severe	6
Major	5
Highly Significant	4
Significant	3
Measurable	2
Negligible	1

For visual clarity, a "traffic light" system is used with Level 1 Risks showing as Green, and Level 6 as Red.

The following grid is calibrated for the Corporate level Risk Register. At Operational and Project level, financial risk should be re-calibrated to reflect the proportionate risk to the total budget. For further information, see section 3.11 below.

Impact and Likelihood				*Used for scoring Gross and Net Risks*						
					Measurement of Impact					
				People	Injuries or ailments not requiring medical treatment.	Minor injury or First Aid Treatment Case.	Serious injury causing hospitalisation or multiple medical treatment cases.	Life threatening injury or multiple serious injuries causing hospitalisation.	Death or multiple life threatening injuries.	Multiple Deaths and Serious Injury
				Reputation	Internal Review	Scrutiny required by internal committees or internal audit to prevent escalation.	Scrutiny required by external committees or ACT Auditor General's Office, or inquest, etc.	Intense public, political and media scrutiny. Eg: front page headlines, TV, etc.	Consistent National Media and Or Inquiry	Government or Commission of inquiry or adverse national media.
				Business Process & Systems	Minor errors in systems or processes requiring corrective action, or minor delay without impact on overall schedule.	Policy procedural rule occasionally not met or services do not fully meet needs.	One or more key accountability requirements not met. Inconvenient but not student welfare threatening.	Strategies not consistent with Government's agenda. Trends show service is degraded.	Widespread Systems failures and client complaints	Critical system failure, bad policy advice or ongoing non-compliance. Business severely affected.
				Financial	<100k	£101k-£500k	£501k-£1m	£1m-£5m	£5m-£15m	>£15m
					1	2	3	4	5	6
					Negligible	**Measurable**	**Significant**	**Highly Significant**	**Major**	**Severe**
Likelihood	>1 in 10	Almost Certain	The event is expected to occur or occurs regularly (highly likely chance)	6	6	12	18	24	30	36
	1 in 10 - 100	Likely	The event will probably occur (significant chance)	5	5	10	15	20	25	30
	1 in 100 – 1,000	Possible	The event may occur (realistic chance)	4	4	8	12	16	20	24
	1 in 1,000 – 10,000	Low	The event could occur (moderate chance)	3	3	6	9	12	15	18
	1 in 10,000 – 100,000	Unlikely	The event may occur in certain circumstances (remote chance)	2	2	4	6	8	10	12
	< 1 in 100,000	Remote	The event is not foreseen to occur or may occur in exceptional circumstances (very remote chance)	1	1	2	3	4	5	6

3.6 CATEGORIES OF RISK

There are a number of recognised categorisations of Risk. The University has adopted the acronym **SORF** (Strategic, Operational, Regulatory and Financial) to categorise its Objectives and therefore the associated Risks.

Strategic	Risk to key institutional aspiration/s
Operational	Risk affecting service/s to staff / students
Regulatory	Risk to meeting legal / statutory responsibilities
Financial	Risk affecting funding

Ideally, each Risk will be allocated to only one category, according to its main criteria. For example, a risk associated with carbon management might be Regulatory or Financial depending on the University's stated Objective.

3.7 RISK MAP

Each Risk will be scored for ***Likelihood*** and ***Impact***, and the results automatically plotted on a Risk Map within the electronic Risk Register document. The Residual or Net Risk score will be used (See 3.8).

3.8 RISK MANAGEMENT AND MITIGATION

Each Risk has a corresponding Risk Action Plan, which will be maintained and updated by the **Risk Owner** or their designated nominee (**Risk Manager**). The Risk Owner is the relevant member of the University Management Group with overall ownership of the associated strategic objective. Within the Colleges Risk Owners' designate nominees with responsibility for updating the Risk Action Plan, for example the College Registrar. The College Registrar act as **Risk Champion** within their College. This satisfies an internal audit recommendation that in addition to having a Risk Register, each College or Department should have a Risk Champion, distinct from the Risk Owner.

The following diagram demonstrates the "flow" from Identification through Assessment and Management:

Within the Risk Action Plan template:

- Risk Background indicates **Inherent Risk Score** *(before mitigating actions are taken)*
- Current Controls indicate **Residual Risk Score** *(in real time, as mitigating actions are taken). This is sometimes referred to as Gross or Net Risk.*

See Appendix for sample Risk Action Plan

Within the Risk Action Plan, a decision has to be taken whether to;

- Transfer
- Treat
- Tolerate or
- Terminate

the activities associated with the Risk. Such decisions will take into account the University's overall Risk Appetite (*see 3.4 above).*

Transfer of a Risk will include consideration of **Insurable Risk** through the Risk Management Committee Sub-Committee.

Treatment comprises mitigating activities which change either the likelihood or the consequences of the risk and any benefits or compromises should be documented within the Risk Action plan. The relative costs and benefits of Treatment must be considered within this decision-making process.

Toleration of a Risk likewise requires consideration of the continuing costs/benefits associated with the activity.

Termination of an activity may occur where the costs (e.g. financial or reputational) significantly outweigh the benefits or where the activity is no longer in line with the University's Strategic Objectives.

Only key controls and improvement actions should be detailed on risk registers. The registers should contain cross-references to detailed process and control documentation if relevant instead of including this in the Risk Action Plan.

For example, while it would be appropriate to reference a plan to relocate lectures in the event of a loss of a single building, under Current Controls, it is not necessary to include the details of that plan within the Risk Action Plan.

Current Actions are typically short-term activities to reduce the likelihood of an event taking place. Once complete, they should be removed from the Risk Action Plan, or moved into Current Controls if relevant. For example, a Current Action might be to draw up a plan to relocate lectures; once that Plan has been drawn up, it becomes a Current Control.

Newly Recommended Actions are those actions proposed at the time of reviewing a Risk. These would be expected to move into Current Actions at the next review date, with a note on progress.

It is recommended that all Actions be allocated a person responsible, ratings for priority and difficulty and a date by which they should be complete, in order to monitor progress and ensure accountability.

It is the responsibility of Risk Managers to monitor progress against agreed completion dates and to alert Risk Owners to any slippage.

Risk Owners are ultimately accountable to the University Court for the management and regular review of their risk/s.

3.9 IMPROVEMENT OPPORTUNITIES

In reviewing the Risk Register, the University will consider opportunities for Improvement using the following grids:

Ability to Manage

Weighting	Description	Explanation
1	Unmanageable external risk	Organisation has (essentially) no ability to influence the risk or its consequences e.g. introduction of new general legislation
2	External risk with limited ability to manage	Organisation has only limited ability to influence the risk or its consequences e.g. introduction of changes to fire service at national level
3	External risk with significant ability to manage	Organisation can influence the impact and/or likelihood of occurrence e.g. arson, computer hacking
4	Internal risk that is not fully manageable	Organisation can largely influence the impact and/or likelihood of occurrence e.g. staff retention, machinery breakdown
5	Internal risk that is essentially fully manageable	Organisation can wholly influence the impact and/or likelihood of occurrence e.g. overspend/ delay on project execution

Effectiveness of Current Controls

Weighting	Description	Explanation
1	Excellent	Mitigation measures at or above global best practice level (independently assessed)
2	Good	Good mitigation measures in place, regularly reviewed and good knowledge by all in activity
3	Average	Formal mitigation measures in place, or part of Standard Operating Procedures
4	Poor	Minimum, or legal minimum mitigation measures in place
5	No Mitigation	No or negligible formal mitigation measures in place

3.10 FREQUENCY OF REVIEW OF UNIVERSITY RISK REGISTER

The University Corporate Risk Register is subject to formal review by the University Operating Board twice per year.

In preparation for this review, the University Management Group will consider updates to the Corporate Risk Register on a regular basis, in line with the annual planning cycle. The frequency with which Risk appears on the UMG agenda will remain flexible, to allow the University to respond to e.g. changes in the funding environment, but is likely to be at least 4 times a year.

As the Register is derived from the University's Strategic Plan, it is closely tied to the University's business objectives for the next one to three years, with associated Key Performance Indicators. Therefore, the evaluation of risks to achieving the University's stated objectives forms an integral part of the annual planning process. Each of the stated objectives is linked to a committee or formal group within the corporate governance structure, and also to an individual (or set of individuals), who is responsible for delivering the objectives and managing the attendant risks, the Risk Owner/s.

3.11 LOCAL RISK ASSESSMENTS

The production of local risk assessments at Project, School, College, and Directorate level is devolved to these areas, using the standard template, with appropriately re-calibrated levels of Likelihood and Impact for financial risk. It is suggested that 1 - 5% of the total budget be considered "Highly Significant", with appropriate values for lower and higher levels of impact:

Severity	Corporate level	As a percentage of total budget, also applicable at Operational and Project levels	Impact
	>£15M	>15%	6 - Severe
	£5M - £15M	15%-5%	5 - Major
	£1M - £5M	5%-1%	4 – Highly Significant
	£501k - £1M	1% -0.5%	3 - Significant
	£101k - £500k	0.5%-0.1%	2 - Measurable
	< £100K	<0.1%	1 - Negligible

College Executive and administrative Directorate Committees (e.g. Estates, Finance, HR) will routinely consider their respective Risk Registers, with Clerks to committee updating the local Risk Registers after each meeting. Any changes made will be traceable to their author and highlighted.

Project-level Risk Registers, using the same template, are reviewed at each Project Board meeting with onward reporting via the Capital Programme Monitoring Group to the University Management Group.

Note: 7/11/14 Forthcoming Project Management Methodology proposes that each Project be given an overall Risk rating. Further information will follow.

Risks may be escalated to the University Register of Strategic Risks by a Head of College or Director through representation on the University Management Group. For example, risks which occur at School-level across a large number of Schools may have a cumulative impact which warrants their consideration for inclusion in the University Corporate Risk Register. Such discussions will occur at College Executives and the University Management Group.

3.12 CENTRAL CO-ORDINATION OF RISK

While Risk Owners will carry responsibility for regular maintenance of "their" Risk Action Plans, it will be the responsibility of the Clerk to UMG *(within Policy, Planning & Governance)* to co-ordinate proposed changes to the Corporate Risk Register, on a (minimum) twice-yearly cycle. For example, Court approved updates to the Corporate Risk Register in June 2013 and again in December 2013. The current timetable for updates is available from the Clerk to UMG, who can also provide guidance on use of the electronic templates.

Each of the stated objectives and risks will be related to a committee or formal group within the corporate governance structure who will be responsible for monitoring the risks, and also to those with direct responsibility for delivering the objectives within the Risk Action Plans and managing the risks (the Risk Owners).

UMG will consider the various risk reports with reference to the institutional stated Key Performance Indicators and Corporate Risk Register. It will also receive Health and Safety Committee risk assessments and reports.

The following flow chart sets out Risk Management Roles and Responsibilities.

4 ROLES AND RESPONSIBILITIES

OPERATING BOARD
Requires assurance of the effectiveness of the University's Risk Management processes and will routinely receive the Risk Register twice a year.

AUDIT COMMITTEE
Requires assurance of the effectiveness of the University's Risk Management processes and will positively receive the Risk Register and regular reports from the Risk Management Committee.

UNIVERSITY MANAGEMENT GROUP
- Will assume a more active role in respect of Risk Management and monitoring the University Register of Strategic Risks.
- Will receive reports from College Executives and the Directors Group, the RISK OWNERS, on risks in their areas of responsibility.
- Will have the power to add or remove risks from the University Register of Strategic Risks.
- Will have Risk Management as a standing item on its agenda.

COLLEGE EXECUTIVES }
DIRECTORS GROUP }
Will hold responsibility for risk in their respective areas, reporting to UMG as necessary, and receiving reports from designated individuals on their constituent Schools/Departments/Sections.
It is expected that some risks will cut across the boundaries of Colleges/Schools/Directorates.

COLLEGE REGISTRARS
Will hold responsibility of administrative co-ordination of risk in their Colleges to include:
- The Role of RISK CHAMPIONS within Colleges;
- Monitoring College-led mitigating actions in the University Register of Strategic Risks;
- Updating the electronic, centrally-held University Register of Strategic Risks;
- Receiving and disseminating feedback to and from Heads of Schools, Directors of Teaching & Learning, and Directors of Research.

UNIVERSITY COMMITTEES /ADVISORY GROUPS
All University Committees and Advisory Groups will have risk as a standing item on their agendas. Clerks will be responsible for notifying risks to contacts in their area (Director/Head of College, etc).

INDIVIDUALS
All members of staff are responsible for the identification and investigation of risk in their areas, reporting upwards through College Registrars/Directorate-designated individuals. Line managers will ensure that all members of staff are aware of the content of local and Strategic Risk Registers.

5 MEASURING THE EFFECTIVENESS OF THE RISK MANAGEMENT PROCESS

5.1 INTERNAL AUDIT

As indicated (*at 2 above*) the Audit Committee must be satisfied as to the University's Risk Management arrangements and will receive the Corporate Risk register at least once per year together with a risk management report from UMG. The Risk Management processes are also subject to review by the University's internal auditors both formally through the internal audit process and through the auditor's reliance on the University Register of Strategic Risks in formulating its 3-year Audit Needs Assessment. The University's External Auditors also take account of the University Corporate Risk Register.

5.2 KEY PERFORMANCE INDICATORS FOR THE RISK MANAGEMENT PROCESS

UMG will regularly review the effectiveness of Risk Management processes..

6 USE OF THE ELECTRONIC TEMPLATES

Risk Owners are responsible for the maintenance of the Risk Action Plan attached to "their" Risks, either personally or by delegation to a nominated individual in their area. Within Colleges, it is proposed that this role be taken on by College Registrars (*see 4 Roles and Responsibilities).*

The Risk Register is an Excel 2007 file which does not retain full functionality in earlier versions of Excel. Template users should therefore contact DIT for a software upgrade and appropriate training if required.

A technical guidance note is attached at Appendix A.

7 REVIEW OF PROCEDURES

These procedures will be reviewed at least every three years. .

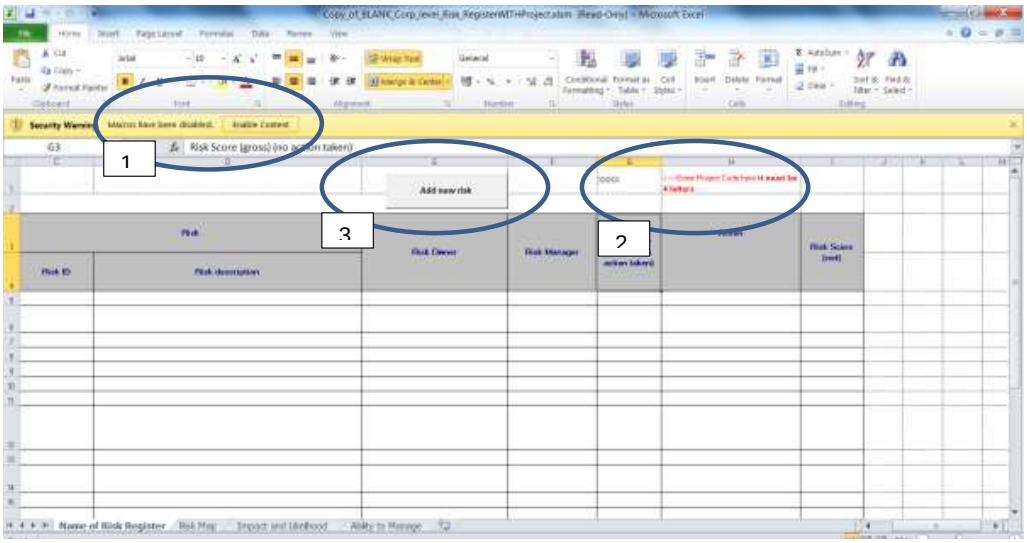
7 November 2014

Appendix A: Technical Guidance for use of the Risk Register Template

A blank template for use at Project or School level is available within staffnet on the University website, under “Risk Management.

Download and save a copy to your PC.

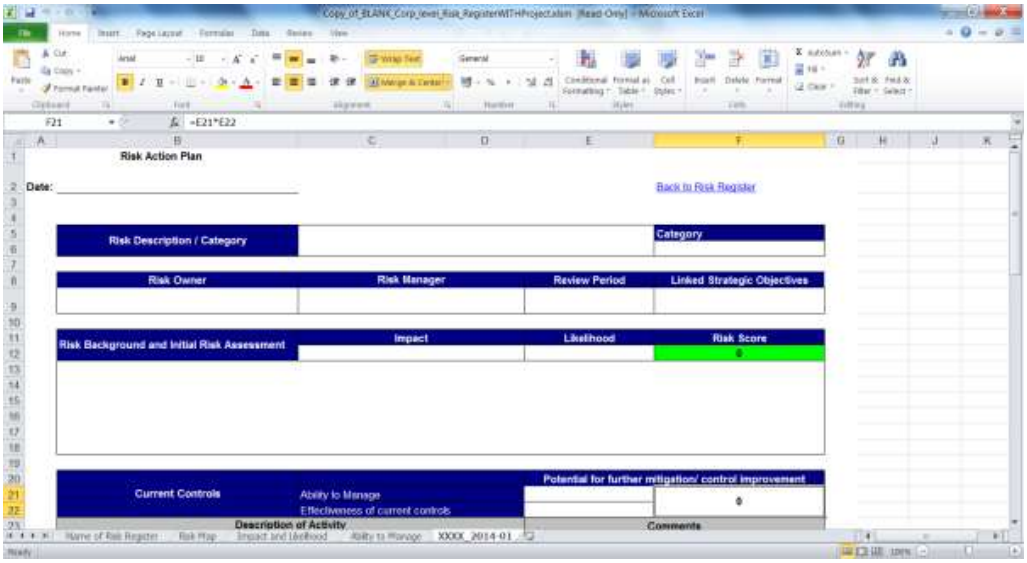
http://www.abdn.ac.uk/staffnet/governance/risk-management-283.php



1 “Enable content” in the yellow toolbar and click “Yes” to “Make this a Trusted Document?” Always remember to enable macros when you open the document.

2 Name your Risk Register with a logical 4-character code, for example “CORP” is used for the CORPorate Risk Register. Enter these 4 digits in cell **G1** as indicated above.

3 Now you are ready to start creating risks!
Click on the grey button “Add New Risk”.



A blank Risk Action Plan (RAP) will appear. It is automatically named “XXXX_year_01” where XXXX is your chosen 4-digit code.

Now follow the main Risk Procedures to complete the RAP.

ALL data should be entered on the RAP and not on the front sheet.

Remember to save your document regularly.

When you have finished your RAP, return to the front sheet, which will now contain the details you entered on the RAP: Risk name, owner and scores.

To add another risk, click “Add New Risk” and a second blank RAP will appear for completion as before.

Important Note: Cells F12 and F41 are vital to the macro function of the template.
Do not add or remove any rows above these cells or the Risk Map will fail to run and your front sheet will not auto-complete.

(METADATA)

APPROVALS	**DATE**
RMC	02.11.2010
UMG	23.11.2010
OB	24.11.2010
Court	29.03.2011
Review by: PPG	05.02.14 7.11.14

Title	Risk Management Policy and Procedures
Author / Creator	Ruth MacLure, Policy Adviser
Owner	Policy, Planning and Governance
Date published / approved	29 March 2011 – University Court
Version	Version 5: 7 November 2014
Date for next review	March 2015
Audience	All
Related documents	Corporate Risk Register
Subject / Description	Policy and procedures for embedding risk management across all University activities and provide a visible and integrated risk management system
Equality Impact Assessment	No
Section	Policy, Planning and Governance
Theme	Governance

N:\Committee Management\University Management Group\2014-11-10\forUMG2014-11-07_update_RM Policy and Procedures.docx