Haute Ecole

Groupe ICHEC - ISC St-Louis - ISFSC

ICHEC
BRUSSELS MANAGEMENT SCHOOL

Enseignement supérieur de type long de niveau universitaire

Les PME belges face à la digitalisation : Quels sont les risques encourus ?

Mémoire présenté par
Lois SANTOS COUTINHO

Pour l'obtention du diplôme de
Master en Gestion de l'Entreprise

Année académique 2016 - 2017

Promoteur :
Madame Anne GOMEZ

Boulevard Brand Whitlock 2 - 1150 Bruxelles

Remerciements

Tout d'abord, je souhaiterais remercier ma promotrice, Anne Gomez, pour le travail de suivi qu'elle a réalisé tout au long de l'écriture de ce mémoire. Je remercie Madame Gomez pour sa disponibilité et pour ses bons conseils.

Je remercie la personne relais, Marie Garcia, pour les conseils donnés lors des discussions de suivi organisées.

Je remercie également ma maître de stage, Sandrine Bastogne, qui m'a aidé à mieux orienter mon sujet et m'a permis de me rendre à un séminaire au sein de l'Institut des Réviseurs d'Entreprises.

Pour terminer, je tiens à remercier les personnes interviewées à savoir : Xavier van Aerssen et Eric Gryson, pour m'avoir accordé un peu de leur temps précieux et avoir répondu à toutes mes questions.

Sommaire

Introduction

Dans une ère où le digital prend une part considérable dans notre société, un important nombre de Petites et Moyennes Entreprises (PME) belges sont sceptiques et n'osent pas procéder à leur transformation ou évolution numérique. Quels sont les risques que les entreprises peuvent être amenées à supporter lors de leur transformation digitale ?

Dans ce mémoire, nous tenterons de définir quels sont les risques pour les entreprises qui adoptent la digitalisation de leurs procédés et de leurs activités. Les risques concernent tant la petite entreprise qui n'utilise que des appareils électroniques connectés que l'entreprise complètement digitalisée. Les différents risques que nous relèverons au long de ce mémoire font partie d'une liste non exhaustive de risques, nous pourrions définir bon nombre de nouveaux risques car il s'agit d'un domaine en perpétuelle évolution.

Nous décomposerons ce travail en trois parties qui faciliteront la compréhension du sujet. La première partie concernera la digitalisation des entreprises belges sans distinction de taille. Toutefois, nous mettrons l'accent sur les performances de nos PME face à celles des grandes entreprises. Au cours de cette partie, nous aborderons la thématique de la digitalisation et son évolution en Belgique mais aussi trois grands axes la concernant, à savoir : la stratégie digitale, les outils de la digitalisation et la législation visant à encadrer cette ère numérique.

Dans la deuxième partie, nous adopterons une attitude d'auditeur financier qui est amené à réaliser des travaux d'audit au sein des entreprises. Nous tâcherons de définir les particularités qui encadrent l'audit d'une infrastructure numérique. Il s'agira donc de toutes les caractéristiques qu'un auditeur « financier » doit prendre en considération sans pour autant être informaticien. Nous déterminerons également les risques qui proviennent de la gestion journalière des entreprises et des différents procédés qui la régissent.

La troisième partie se verra plus pratique, nous réaliserons un audit des processus financiers digitalisés au sein d'une fiduciaire. Le but n'est pas de certifier les comptes annuels de l'entreprise et d'émettre une opinion positive ou négative, il s'agit de mettre en exergue les différents risques auxquels l'entreprise est soumise.

Partie 1 : La digitalisation des entreprises belges

Nous essayerons tout d'abord de comprendre ce qu'est la digitalisation et les avantages qui y sont liés. Nous développerons également quelques outils qui sont disponibles sur le marché et qui permettent la digitalisation des entreprises. Nous tenterons également de relever les points qui font qu'une entreprise devrait penser à se digitaliser et comment elle devrait procéder pour ce faire.

Le but de cette partie est donc de comprendre le phénomène digital tout en déterminant le cadre législatif qui l'encadre. C'est pourquoi nous aborderons également une loi que la Belgique a introduite afin de réguler le digital au sein des entreprises.

1. La digitalisation

1.1. Définition et avantages

Ce phénomène consiste en la transformation d'un outil, un processus ou même un métier en un code informatique et cela dans un but de pouvoir le remplacer pour en tirer une meilleure performance. Nous avons assisté à la naissance de ce phénomène lors de l'apparition d'internet, par exemple : les courriers postaux ont été remplacés par les e-mails, les forums sur internet ont remplacé certains salons, les sites de e-commerce ont fait leur apparition. Depuis ces événements, nous sommes dans une phase de digitalisation où nous assistons au développement de caisses automatiques dans les supermarchés ou encore la communication au travers de réseaux sociaux comme Facebook par exemple. Il s'agit d'un phénomène dit « naturel » créé de la relation entre internet et les avancées technologiques constantes. (Alphalives, 2017)

« La digitalisation c'est un ensemble de mesures prises par les entreprises pour :

- Gagner du temps dans leurs process ;
- Mieux communiquer entre les différents métiers ;
- Se rapprocher des clients et les fidéliser ;
- Améliorer les conditions de travail des employés ;
- Améliorer le chiffre d'affaire et les marges dégagées ;
- Collecter et traiter toutes les informations bénéfiques à leur performance. » (Conrad, 2016)

Il y a des avantages qui sont liés à la digitalisation. Cette dernière permet de dégager des opportunités dans tous les secteurs, et ce, de diverses façons :

- Nous oublions la notion de « distance », l'information est en mouvement et n'est pas soumise à des contraintes géographiques ;
- Nous atteignons un échantillon plus large de personnes grâce à cette information et les différents contenus dématérialisés ;
- Nous avons la possibilité de travailler sur un projet identique avec d'autres personnes et ce en temps réel, grâce à du contenu partageable et modifiable ;
- Gain de temps de travail grâce à l'automatisation des activités répétitives ;
- Nous pouvons également limiter les erreurs éventuelles. La digitalisation permet de détecter plus facilement les problèmes que rencontre l'entreprise et de les corriger. (Alphalives, 2017)

1.2. Avantage concurrentiel pour les entreprises numériques

Beaucoup d'entreprises considérées traditionnelles se plaignent de concurrence déloyale venant des plateformes numériques. Le résultat ne doit pas être une interdiction d'exercer pour des entreprises comme Uber, Airbnb ou d'autres encore. L'apparition de telles sociétés a fait en sorte que de nombreux secteurs plus « figés », par des règles trop strictes par exemple, se sont retrouvés secouées. (De Leus, 2017)

Il faut reconnaitre toutefois que les entreprises qui se sentent menacées ont leurs raisons de le penser et ont raison sur certains points. Prenons l'exemple d'Uber : les chauffeurs d'Uber ne sont pas redevables d'une Taxe sur la Valeur Ajoutée (TVA) à 6% contrairement aux chauffeurs de taxi traditionnels. Les chauffeurs d'Uber ont la qualification de petite entreprise et font en sorte que leur chiffre d'affaires annuel ne dépasse pas les 25.000 euros[1] (la plupart des chauffeurs Uber exerçant cette activité à temps partiel). Ne dépassant jamais le seuil, cette activité complémentaire permet aux chauffeurs Uber d'avoir un avantage concurrentiel par rapport aux chauffeurs de taxi traditionnels. (De Leus, 2017)

[1] Régime de franchise de la taxe pour les petites entreprises

1.3. La transformation digitale des entreprises

Nous devons tout d'abord comprendre ce qu'une entreprise doit transformer et pourquoi elle doit le faire.

Comme nous le développerons dans un des points suivants, une entreprise qui veut mener à bien sa digitalisation devra songer à mettre en place une stratégie digitale. Il s'agit d'une stratégie comprenant l'entièreté des processus au sein de l'organisation, c'est-à-dire de la récolte d'informations jusqu'à la mise en place de sous-stratégies. La stratégie digitale sera le cœur de l'entreprise, sans elle il sera très difficile pour l'entreprise de mener à bien sa transformation. (Gonzalez, 2016)

Une digitalisation qui est là pour durer dans l'entreprise s'acquiert par la transformation de différentes technologies et catégories conjointement. « Elle touche notamment le modèle d'affaires, la structure de l'entreprise, le capital humain, les processus, la capacité et les compétences, l'offre de produits et services, l'engagement avec les parties prenantes, ainsi que les accélérateurs de la transformation. Il s'agit d'un processus d'amélioration continu puisqu'une stratégie digitale doit continuellement être adaptée pour permettre de saisir les nouvelles opportunités. » (Gonzalez, 2016, para. 4)

La transformation semble être la norme pour toute entreprise désirant s'accaparer le marché et pouvoir faire face à la concurrence croissante de plateformes ou même de concurrents plus innovants. Cependant, la transformation instaure une peur auprès des Petites et Moyennes Entreprises.

La digitalisation représente, en soi, un phénomène complexe. Il s'agit d'un projet intégral qui vient bouleverser les entreprises dans leurs méthodes de fonctionnement. « Elle oblige les dirigeants à mener une réflexion profonde à la fois sur leur culture d'entreprise, leur organisation, leurs investissements financiers ou encore leur structure même. » (Abilways Digital, 2016, para. 4). Il s'agit donc d'une étape complexe et qui se fait sur de nombreuses années. De plus, les Petites et Moyennes Entreprises sont submergées par les impacts de la digitalisation tant en matière de moyens financiers que de moyens techniques et humains. (Abilways Digital, 2016)

L'impact de la digitalisation peut être différent d'une entreprise à l'autre, il peut provoquer la création d'une logistique inédite ou une réorganisation des rôles des membres de l'organisation. Ce qui fait apparaître cette transformation digitale comme étant un travail laborieux amenant des chamboulements qui peuvent causer un rejet de l'application du digital au sein de l'entreprise. (Abilways Digital, 2016)

Le frein principal à la transformation digitale paraît être l'utilisation des outils de la digitalisation. L'écart se creuse entre les PME et les grandes entreprises par rapport à ce point : les grandes entreprises ont plus facile à adopter des nouvelles technologies telles que le cloud computing alors que les petites entreprises peuvent se sentir perdues vis-à-vis de la complexité et des coûts qu'entraîne l'utilisation des outils digitaux que le marché met à disposition. (Abilways Digital, 2016)

Il existe encore deux freins à la digitalisation qui sont :

- La peur de l'échec
- Le manque de connaissances et de formation

Dans les petites entreprises, nous pouvons remarquer que cette peur de l'échec est plus présente car les répercussions sont plus importantes au sein d'une organisation qui n'a pas autant de moyens de financement et de capital. Le dirigeant d'une PME va plutôt calculer ses bénéfices sur le court-terme afin de garantir sa continuité.
Lorsqu'une entreprise décide de se lancer dans une transformation digitale, elle doit tout d'abord prévoir l'intégration de formations fondamentales et efficaces sur les points clés du digital. Nous pouvons en citer quelques-unes qui font partie des formations les plus appropriées pour les PME :

- « La culture digitale permet à l'ensemble des collaborateurs de développer sa culture et ses compétences numérique.
- Développer une posture de manager agile parce que la transformation digitale commence par la transformation des managers pour accélérer la digitalisation et l'innovation au sein de l'entreprise.
- Les fondamentaux des réseaux sociaux pour investir correctement un des canaux les plus efficace du marketing digital.

- Les bases de communication digitale pour optimiser vos investissements et réaliser des campagnes qui permettront de développer votre chiffre d'affaires. » (Abilways Digital, 2016, para. 10)

1.4. Plateformes ou sociétés de services

Une des questions qui se pose est de savoir si les différentes plateformes numériques que l'on connaît constituent plus qu'une simple plateforme qui met en contact différentes personnes pour un service particulier. La Cour Européenne de Justice devrait rendre sa décision concernant le régime fiscal qui doit être appliqué à ce genre d'entreprise. En juillet 2015, le cas Uber a été renvoyé devant la Cour Européenne de Justice par un juge espagnol (Valero, 2016). La Cour Européenne de Justice devrait rendre sa décision vers mi-2017.

Si la Cour Européenne de Justice les considère comme étant de simples plateformes commerciales, alors dans notre exemple, les chauffeurs Uber pourront continuer le système actuel et donc ne pas appliquer de TVA. À l'inverse, si la Cour donne un avis défavorable envers la plateforme d'Uber, cette dernière sera considérée comme un service de transport et devra suivre une réglementation plus sévère.

1.5. Le digital au niveau européen

La nouvelle réalité digitale fait que des décisions doivent être prises au niveau européen. Il faut adapter les anciens modèles tant sociaux qu'économiques. Il semblerait que des milliards d'impôts disparaissent chaque année, et ce grâce à l'évasion fiscale. Il faut mettre un terme à des dispositifs qui permettent à des entreprises de se soustraire au paiement d'impôts ou du moins payer un minimum d'impôts, comme l'a fait Apple en 2014 en ne payant que 0,005% d'impôt en Irlande sur les bénéfices qu'elle avait tiré des activités européennes. (De Leus, 2017)

La Commission européenne propose l'établissement d'une base taxable unique pour l'impôt des sociétés. Cette proposition est connue comme étant le « Common Consolidated Corporate Tax Base » et devrait être une des solutions possibles afin de taxer de manière équitable les grandes multinationales là où les frontières n'existent plus grâce au numérique. (De Leus, 2017)

Du fait qu'il n'y ait plus réellement de frontières, nous pouvons nous attendre à ce que certaines entreprises profitent du système et exercent une concurrence déloyale ou bien évitent de payer certains impôts. Lorsque nous citons « entreprises qui profitent du système », nous faisons référence aux entreprises où le doute est possible entre sociétés de services ou simples plateformes numériques qui mettent en relation des personnes comme dit précédemment dans le point 4.3.

L'importance de l'intervention d'un plan comme le Common Consolidated Corporate Tax Base (Assiette Commune Consolidée pour l'Impôt sur les Sociétés) pourrait être une solution envisageable. Il s'agit d'un ensemble de règles qui permettent de déterminer le résultat imposable d'une société dans l'Union Européenne. Les entreprises qui ont des activités transfrontalières doivent s'accorder sur un système européen unique afin de définir leur revenu imposable, et ne doivent donc pas se référer aux différents régimes nationaux des pays dans lesquels l'entreprise exerce ses activités. (European Commission, 2017)

Cependant, nous pouvons constater que le point de départ sera de définir clairement le statut des entreprises. Trouvons-nous en face d'une entreprise qui preste un type de service ou bien une entreprise qui sert tout simplement d'intermédiaire ? Il faudrait que les contrôles soient plus présents pour s'assurer que les entreprises respectent leur « activité », c'est-à-dire veiller à ce qu'elles ne dépassent pas les seuils par exemple (comme le cas des chauffeurs Uber qui ne peuvent pas dépasser 25.000 euros de chiffre d'affaires).

À partir du moment où une entreprise dépasse les seuils ou exerce des activités qui sont différentes de celles pour lesquelles elle a été créée, les sanctions devraient être plus ou moins graves en fonction du degré de l'infraction. S'il s'agit simplement d'une croissance des activités et qu'aucune infraction n'a été commise, nous pourrions envisager une redéfinition claire et précise des activités de l'entreprise. A contrario, s'il s'agit d'une intention frauduleuse de se soustraire à un quelconque régime d'impôt la sanction devrait être plus lourde allant d'une amende minimum à la cessation des activités forcées si l'infraction est plus grave.

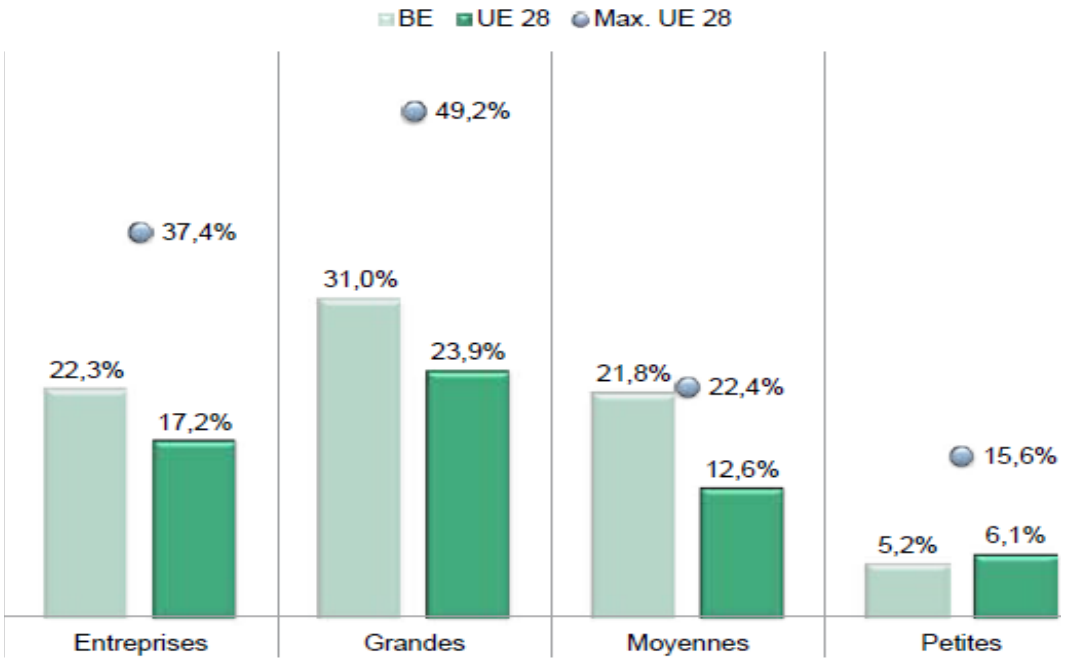
2. L'évolution numérique belge

Afin d'apprécier l'évolution digitale en Belgique, nous allons analyser les chiffres clefs relatifs à cette évolution. De nombreuses sociétés aujourd'hui ont recours à la numérisation de leur activité. L'utilisation des Technologies de l'Information et de la Communication (TIC) se fait de plus en plus présente dans les différentes sociétés sur le marché belge. Ceci se fait grâce, notamment, au développement des nouvelles technologies informatiques mais aussi grâce à internet et aux différents moyens électroniques et digitaux dont dispose l'économie actuelle.
Nous allons tout d'abord analyser les chiffres concernant le commerce en ligne, l'accès à internet et l'utilisation d'une page internet. Il s'agit des trois premiers outils qui servent à la digitalisation des activités des entreprises.

De nos jours, les entreprises belges réalisent leur chiffre d'affaires en partie grâce à des technologies digitales. Pas moins de 22,3 % du chiffre d'affaires d'entreprises qui ont leur activité en Belgique résulte du commerce électronique. Toutefois en fonction de la taille de l'entreprise, la part du chiffre d'affaires qui tire sa source dans l'e-commerce est plus ou moins importante : les petites entreprises ont plus de mal et donc leur part de chiffre d'affaires est six fois moins élevée que dans les grandes entreprises, 5,2 % contre 31 %. (SPF Economie, 2016)

Il y a tout de même une légère amélioration du côté des petites entreprises puisque de 2014 à 2015 la part de chiffre d'affaires a doublé, elle est passée de 2,4 % à 5,2 %. Les petites entreprises belges sont toujours à la traine par rapport au reste de l'Europe dont la moyenne est de 6,1 %. (SPF Economie, 2016)

Graphique 1 : Pourcentage du chiffre d'affaires total des entreprises réalisé par le commerce électronique



Source : SPF Economie – DG Statistique – Statistics Belgium, Eurostat (2015). *Enquête 'Utilisation des TIC et de l'e-commerce dans les entreprises'*. Récupéré de http://statbel.fgov.be/fr/binaries/Barometre_de_la_societe_de_l_information_2016_tcm326-278973.pdf, p. 16.

Dans le cas du commerce en ligne (e-commerce), les entreprises ont besoin d'un accès internet afin de pouvoir réaliser du chiffre d'affaires. L'internet est, pour les entreprises, un outil essentiel dans la gestion de leurs activités. Grâce à cela, le développement de leur réseau est sans frontières. Toute entreprise voulant atteindre un plus grand nombre de personnes à travers le monde peut désormais le faire et ce en un seul clic.

L'accès internet est accessible à (presque) toutes les entreprises belges désormais. Il n'y avait que 1,2 % des petites entreprises qui n'avait pas encore accès à internet en 2015 contre 3 % en 2014 (SPF Economie, 2016). Aujourd'hui, 2017, il est très rare de voir une entreprise qui ne soit pas « connectée » au réseau internet. L'accès à internet est devenu indispensable dans le développement des activités d'une entreprise, à tel point que toute société doit s'aligner afin de rester concurrentielle.

Il faut s'avoir aussi qu'en Belgique, huit entreprises sur dix (81,1 %) possèdent une page ou un site web, mais seulement deux entreprises sur dix (20,8 %) ont reçu des commandes électroniques sur leur site (SPF Economie, 2016). Nous pouvons supposer que ces chiffres seront revus à la hausse pour l'année 2016, du simple fait que les mentalités changent et que

la plupart des consommateurs d'aujourd'hui font leurs achats en ligne pour de nombreux articles. Désormais, tout est accessible sur internet ; nous faisons nos courses sur internet, nous achetons nos vêtements sur internet, nous réservons nos billets d'avion sur internet, etc. L'outil est fait de telle sorte, qu'il nous permet d'avoir une multitude de services et biens divers sans avoir à se déplacer et à fournir le moindre effort.

En 2015, il y avait 8 % des entreprises ayant leur activité en Belgique qui acceptaient les paiements en ligne pour l'achat de biens ou services sur leur site web (ou via des applications de paiement), contre 12,7 % qui ne l'acceptaient pas. (SPF Economie, 2016)

3. La stratégie digitale

Dans les deux points précédents, nous avons procédé à une première approche du digital. Nous avons fait le point sur les avantages, les freins et les raisons pour lesquelles une entreprise devrait songer à la digitalisation de ses activités. La digitalisation de tout ou d'une partie des activités est une étape importante de la vie d'une entreprise et celle-ci ne peut pas être menée sans une préparation préalable de la part des membres de l'organisation. Il est important que l'entreprise pense à sa « stratégie digitale » et aux politiques liées à celle-ci. Une stratégie est donc indispensable pour que l'entreprise puisse se préparer correctement à sa « transformation ». Nous pourrions être amenés à penser que la digitalisation ne touche que les entreprises technologiques mais ce n'est pas le cas ! Peu importe le domaine dans lequel l'entreprise exerce son activité, elle est impactée par la digitalisation. On retrouve de nombreux secteurs, notamment :

- Les fiduciaires ;
- Les banques ;
- Les entreprises industrielles ;
- Etc.

Les entreprises doivent dorénavant tenter d'aboutir à une stratégie digitale, ainsi elles acquerront des nouvelles connaissances et une nouvelle façon de faire afin de rester compétitives (MBD Consulting, 2016). Une entreprise qui laisse la concurrence se digitaliser, et ne se digitalise pas elle-même, perd du terrain face à la concurrence. Toutefois, une

entreprise qui se digitalise sans penser à une stratégie afin de mener à bien le processus de digitalisation encourt tout autant de risques de voir sa digitalisation échouer.

La numérisation impacte donc le fonctionnement d'une entreprise, que ce soit au niveau de la communication, au niveau de son management, au niveau des ressources humaines ou encore au niveau de sa production. Les entreprises doivent garder à l'esprit que cette digitalisation nécessite une attention particulière, il ne faut pas la traiter comme une activité banale. Elle doit être intégrée dans la stratégie d'entreprise (MBD Consulting, 2016).

3.1. Qu'est-ce qui doit être repensé ?

L'entreprise doit donc repenser tous les processus qu'elle a mis en place, de la récupération des informations importantes à la mise au point de stratégies nouvelles ou sous-stratégies. Cette stratégie sera le core de l'entreprise. On parle également de digitalisation durable d'une entreprise qui consiste en réalité à la transformation simultanée de plusieurs catégories et technologies au sein de l'entité.

Cette transformation touche entre autres :

- La structure de la société :
    - Il faut, par exemple, penser à de nouveaux postes à pourvoir. Notamment des postes liés aux nouvelles technologies que l'entreprise se verrait acquérir.
- Le modèle d'affaires :
    - Une entreprise qui vend uniquement en magasin doit songer à créer un site internet et réaliser de la vente en ligne.
- Le personnel :
    - La digitalisation peut amener une restructuration parmi les membres du personnel avec notamment des licenciements mais pas forcément ! Il se peut également que l'entreprise donne l'opportunité au personnel de suivre des formations afin de ne pas se laisser dépasser par les nouveautés.
- Les processus :
    - L'entreprise peut être amenée à modifier certains processus ou à donner naissance à des nouveaux. L'entreprise devra notamment penser à des processus de contrôle des applications ou des personnes utilisant les nouveaux outils.

- Les différents produits et/ou services :
    - L'entreprise pouvant atteindre une panoplie de clients devra prendre en considération les attentes des nouveaux marchés qui apparaissent grâce à la disparition des frontières que permet internet.

Il faut encore que cette stratégie soit continuellement améliorée pour que l'entreprise puisse saisir toutes les opportunités qui se présentent à elle. (MBD Consulting, 2016)

Comme l'environnement digital change vite, l'entreprise a besoin de s'adapter assez rapidement aussi. Ceci entraîne donc que la stratégie soit constamment présente dans la gestion journalière de l'entreprise, ce qui était d'application hier ne l'est plus forcément aujourd'hui. Prenons l'exemple des factures. D'abord, nous avons assisté à l'envoi de factures électroniques qui ne permettaient pas un traitement informatique afin d'extraire les informations, aujourd'hui cela est désormais possible.

Prenons le cas d'Excellium Solution SPRL, la fiduciaire dont nous réaliserons l'analyse de risques en troisième partie. Le cabinet utilise, depuis quelques années maintenant, un logiciel qui permet de traiter les factures et qui propose un encodage automatique. Grâce à la dématérialisation – procédé permettant de faire passer un document au support physique sous un format électronique – des factures, l'attribution d'une pièce comptable à une écriture comptable est possible. Ce logiciel permet donc à l'entreprise de gagner du temps lors de l'encodage puisque le logiciel propose une écriture qui, si elle convient au comptable, ne doit plus qu'être validée.

Cela fait partie des évolutions technologiques que l'entreprise doit prendre en compte afin d'améliorer constamment sa stratégie digitale et la maintenir à jour.

3.2. Définir sa stratégie digitale

La création de cette stratégie se fait en cinq étapes (MBD Consulting, 2016, para. 8) :

1. « La collecte de données et d'informations
2. L'évaluation de l'*écosystème* digital existant
3. La planification des nouvelles ressources
4. L'identification des risques potentiels
5. La priorisation des choix stratégiques et intégration des ressources digitales »

La collecte des informations permet d'avoir une image claire et complète des ressources digitales déjà présentes au sein de l'entreprise. Une fois que ces-dernières sont définies, la société va pouvoir déterminer quelles sont les différentes opportunités qui s'offrent à elle. L'organisation terminera cette étape en définissant des indicateurs clefs de performance par rapport à chacune des ressources existantes.

« Par définition, un écosystème est un ensemble dynamique d'acteurs qui interagissent entre eux dans un environnement donné. L'écosystème numérique regroupe donc différents acteurs du digital dans une optique d'échanges et de partages, en vue de développer l'environnement numérique.
Ainsi, il existe plusieurs écosystèmes numériques car un écosystème peut être local, régional, national ou encore, n'être présent que sur un marché défini. » (Cardoso, 2016, para. 4)

Le but de l'évaluation de l'écosystème digital existant est d'acquérir une compréhension globale de l'état des différentes ressources présentes et connaître également la performance de celles-ci face à celles dont disposent les concurrents de l'entreprise. L'organisation cherchera donc à découvrir quels sont les moyens qui sont mis à sa disposition pour qu'elle puisse améliorer son efficacité digitale et ne pas être trop à la traîne.

3.3. Mettre en place sa stratégie digitale

Une fois que l'entreprise a identifié les différents points repris ci-dessus, elle peut passer à l'implémentation de sa stratégie qui comprend, elle aussi, cinq étapes (MBD Consulting, 2016, para. 9) :

1. Définition d'un plan d'action
2. Mise en place de mesures de performance
3. Surveillance et amélioration continue de l'expérience utilisateur et client
4. Choix du responsable de la stratégie digitale
5. Compréhension de la dette technique

La définition d'un plan d'action va entraîner une réorganisation de la chaine de valeur et une nouvelle conception de l'offre pour pouvoir profiter de nouvelles opportunités de développement de produits. Choisir un responsable de la stratégie digitale va affecter l'intégralité de l'entreprise car tous les départements qui composent l'organisation vont jouer

un rôle essentiel dans le succès futur de la stratégie digitale. Lorsque l'on parle de dette technique, il faut prendre en considération le coût de la dette. Il s'agit en fait des coûts supplémentaires qui sont liés à une mauvaise mise en place ou gestion des activités digitales. (MBD Consulting, 2016)

Définition de la dette technique :
« (…) La dette technique représente tous les éléments logiciels (code, test, doc, archi, …) non terminés ou dépassés et qui sont du coup imparfaits. Il faudra donc très certainement les corriger sous peine de souffrir gravement de leurs défauts. » (Blanc, 2016, p. 3)

Lorsque nous prenons le temps d'analyser les différents éléments présentés ci-dessus, nous constatons que l'intégration d'éléments digitaux dans une entreprise est un réel souci au sein d'une entreprise qui va bouleverser sa façon d'être et sa façon d'agir. Il s'agit ici d'un des facteurs clefs qui perturbent encore les dirigeants des PME belges. Ce n'est pas tellement le fait de devoir repenser à une nouvelle stratégie qui les inquiète, car une entreprise est constamment amenée à devoir améliorer sa stratégie. Ce qui peut leur paraitre le plus inquiétant, est de devoir songer à une nouvelle stratégie comportant des éléments dont ils ne détiennent pas forcément le contrôle ! C'est notamment le cas du cloud dont nous parlions dans le premier chapitre.

Les mentalités doivent certes évoluer et le digital est effectivement le futur de nos entreprises, mais il faut être conscient que l'implémentation d'une stratégie digitale doit être réalisée consciencieusement et chaque détail concernant cette dernière doit être évalué correctement.

3.4. Mettre en place une politique de sécurité du numérique

Comme nous le disions lors de l'introduction du point 3, l'entreprise doit mettre en place une stratégie mais également des politiques. Une des politiques essentielles en matière de numérique est celle de la sécurité, nous allons voir ce qu'elle représente et à quelle point elle est présente dans nos entreprises belges.
La sécurité numérique d'une entreprise représente la capacité de cette dernière à protéger tous les éléments numériques en son sein. Cela reprend donc toutes les mesures prises afin de protéger les données sensibles qui sont sur le réseau internet et que l'organisation traite. En dehors des données sensibles, il s'agit aussi de protéger tous les outils informatiques utilisés

par l'entreprise, comme par exemple protéger les ordinateurs par des anti-virus ou encore la définition de logins et de mots de passe que l'entreprise pour les différentes applications.

Le baromètre de la « société de l'information 2016 » du SPF Economie expose les différents problèmes rencontrés par les personnes physiques et morales lorsqu'ils sont sujet au numérique. En 2015, 32 % de nos entreprises avaient défini une politique de sécurité des TIC (SPF Economie, 2016). Toujours selon le baromètre, il s'agit d'une politique qui est beaucoup plus présente dans les grandes entreprises à raison de 73 % contre 28 % des petites entreprises.

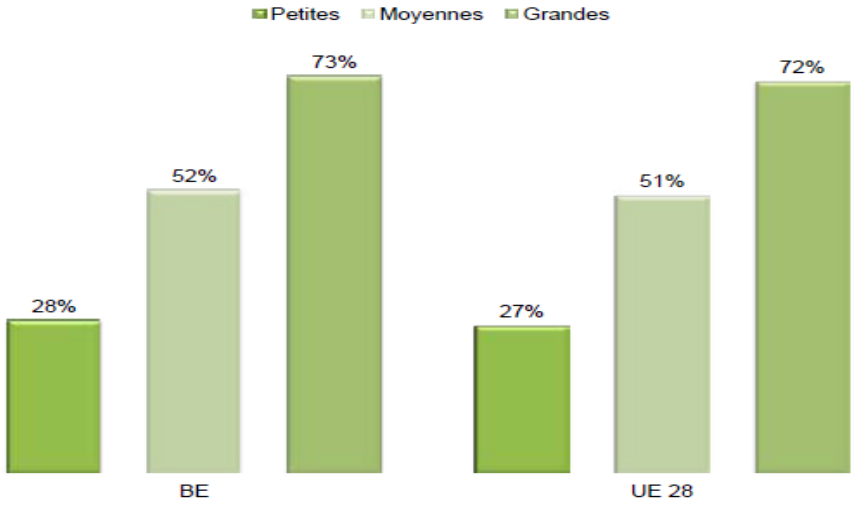
Une politique de sécurité des systèmes d'information est constituée de documents qui préconisent des règles de sécurité que les membres d'une organisation doivent appliquer et respecter. Cette politique est liée à une démarche générale qui va de pair avec la politique de l'organisation en matière d'amélioration continue. (Université Grenoble Alpes, 2017)

L'Université Grenoble Alpes a mis en place une politique de sécurité des systèmes d'information qui regroupe deux documents indispensables :
« Le document « Politique générale de sécurité des systèmes d'information » exprime les enjeux et les grands objectifs de sécurité, propose les mesures organisationnelles et techniques pour atteindre les objectifs de sécurité ciblés.
Le document « Politique de management de la sécurité de l'information » qui précise quant à lui l'organisation des instances de pilotage et des acteurs de la sécurité des systèmes d'information. » (Université Grenoble Alpes, 2017, para. 3)

Les documents repris ci-dessus sont propres à l'université, cependant le principe reste le même pour les autres entreprises. Chaque entreprise peut définir une politique de sécurité numérique propre à son domaine d'activités. Nous dirons « peut » car cela ne constitue pas une obligation légale. Cependant, nous conseillerons fortement l'établissement d'une politique en vue d'éviter certains risques liés à la sécurité comme par exemple le risque d'hacking car la sécurité digitale est trop faible.

Dans le tableau qui suit, nous pouvons observer combien d'entreprises (de toutes tailles) ont pensé à l'instauration d'une politique de sécurité.

Graphique 2 : Pourcentage des entreprises qui ont mis en place une politique de sécurité des TIC



Source : Eurostat. (2015). *Enquête 'utilisation des TIC et de l'e-commerce dans les entreprises'*. Récupéré de http://statbel.fgov.be/fr/binaries/Barometre_de_la_societe_de_l_information_2016_tcm326-278973.pdf, p. 77.

La sécurité du numérique est l'affaire de toutes les entreprises quelles qu'elles soient. Il est primordial pour toute entreprise de garantir une sécurité de l'information qu'elle traite. De nombreuses entreprises de services, principalement les entreprises de conseil, de comptabilité, les avocats, les notaires, les banques, détiennent des informations privilégiées sur leur clientèle. Le combat d'aujourd'hui est de pouvoir garantir la sécurité de toute cette information.

La digitalisation des entreprises, pour être mise en place de manière efficace, doit être accompagnée d'une stratégie bien définie. Les entreprises qui prévoient d'utiliser des processus digitaux, doivent prendre des précautions. La question doit être longuement étudiée afin d'éviter tout problème futur car les paramètres connexes n'auront pas été clairement définis et pris en considération. Les paramètres connexes représentent non seulement toutes les « configurations programmes » pour une bonne utilisation des logiciels, mais ils représentent également la détermination des personnes responsables des différents processus (comme nous l'avons vu dans l'exemple de l'université de Grenoble).

Les différents problèmes auxquels les sociétés sont confrontées sont de tous types, en voici quelques exemples :

- Cybercriminalité ;
- Fraude par internet ;

- Perte de données ;
- Confidentialité.

Les différents problèmes repris ci-dessus sont bien connus de tous, le fait est que ces problèmes ne vont cesser de s'accroître si des mesures ne sont pas prises pour les contrer. Il va falloir prendre en considération les différents risques qu'encourent les entreprises et quels sont les moyens dont elles disposent pour les éviter.

4. Les outils de la digitalisation

Pour pouvoir se digitaliser, une entreprise a différentes possibilités. En fonction de son activité, de ses objectifs ou du secteur dans lequel elle se trouve, l'entreprise va faire appel à différents outils. Le choix est plutôt vaste et les formes de digitalisation sont variées : nous pouvons passer de la simple utilisation d'un logiciel comptable au travail en cloud ou encore à l'automatisation d'activités.

Nous n'aborderons pas la totalité des formes de digitalisation mais développerons celles qui nécessitent une compréhension pour la suite de ce mémoire et pour la réalisation de l'analyse de risques.

Afin de préparer le cas pratique, nous analyserons ce qu'est le cloud computing et les éléments issus des Technologies de l'Information et de la Communication (plus précisément de la facture électronique et des logiciels favorisant la communication informatisée). Ces éléments sont également liés à la seconde partie de ce mémoire car nous y développerons l'audit financier en milieu informatique, ce qui nécessite donc une compréhension de ces éléments.

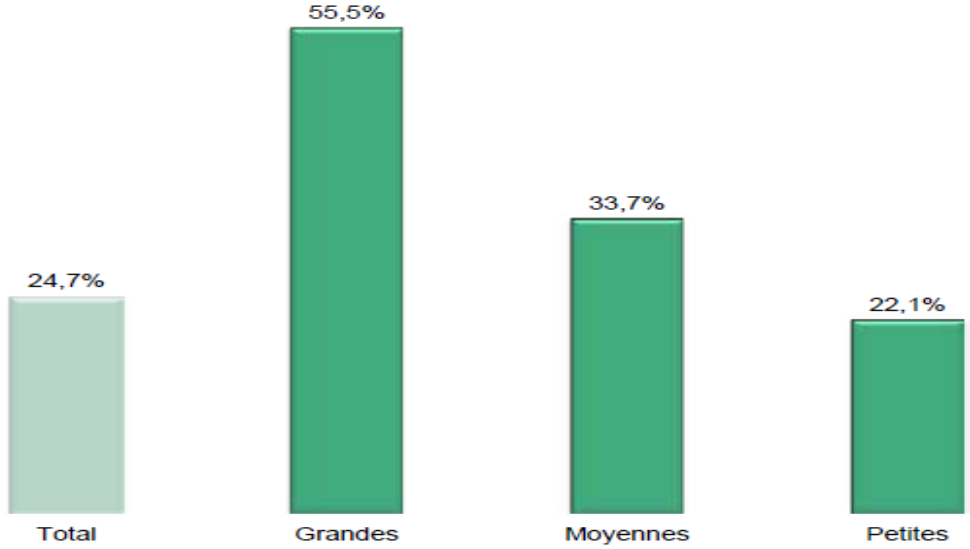
4.1. Cloud computing

« Le Cloud Computing est un terme général employé pour désigner la livraison de ressources et de services à la demande par internet. Il désigne le stockage et l'accès aux données par l'intermédiaire d'internet plutôt que via le disque dur d'un ordinateur. Il s'oppose ainsi à la notion de stockage local, consistant à entreposer des données ou à lancer des programmes depuis le disque dur. » (Bastien, 2017, para. 2)

En 2015 une entreprise belge sur quatre faisait appel aux services de cloud computing environs 24,7 % des entreprises. Il s'agit d'une petite progression face à l'année antérieure qui était de 21,2 % (SPF Economie, 2016). Ce que nous pouvons relever ici, c'est que l'augmentation n'est pas des plus marquantes. Nous constatons une réticence de la part des dirigeants d'entreprises face à l'utilisation du cloud. Cette réticence est, peut-être, due au fait que l'entreprise ne détient pas le contrôle exclusif sur le serveur, ce qui représente un risque pour l'entreprise comme nous le verrons par la suite dans ce mémoire. Il ne s'agit pas de l'unique risque lié au cloud computing. D'autres risques seront observés et analysés dans la suite de ce mémoire.

Encore une fois, l'utilisation du cloud computing varie en fonction de la taille de l'entreprise. Les petites entreprises sont encore à la traîne par rapport aux grandes : 22,1 % pour les petites contre 55,5 % pour les grandes (SPF Economie, 2016).

Graphique 3 : Entreprises achetant des services de cloud computing



Source : SPF Economie – DG Statistique – Statistics Belgium. (2015). *Enquête 'Utilisation des TIC et de l'e-commerce dans les entreprises'*. Récupéré de http://statbel.fgov.be/fr/binaries/Barometre_de_la_societe_de_l_information_2016_tcm326-278973.pdf, p. 36.

Dans le tableau qui suit, nous pouvons mettre en exergue quels sont les différents services auxquels les entreprises souscrivent lorsqu'elles font appel à du cloud computing.

Tableau 1 : Différents services payants du cloud computing dans les entreprises

(en % des entreprises utilisant des services payants de cloud)	2014	2015
Stockage de fichiers	61,5	61,5
Courriel	52,5	59,0
Hébergement de base(s) de données de l'entreprise	45,4	48,6
Logiciels de comptabilité	33,3	44,1
Logiciels de bureautique	31,2	29,7
Gestion de la relation client (CRM)	26,2	32,8
Puissance de calcul pour faire fonctionner les logiciels de l'entreprise	23,0	31,8

Source : SPF Economie –DG Statistique – Statistics Belgium. (2014-2015). *Enquête 'Utilisation des TIC et de l'e-commerce dans les entreprises'*. Récupéré de http://statbel.fgov.be/fr/binaries/Barometre_de_la_societe_de_l_information_2016_tcm326-278973.pdf, p. 36.

Comme nous pouvons le constater, au top des services auxquels les entreprises souscrivent nous retrouvons le stockage de fichiers. La variation n'est pas tellement grande entre 2014 et 2015, mais nous remarquerons que les logiciels de comptabilité ont progressé de 9 % environ. Une pratique qui se répand de plus en plus.

4.2. Les Technologies de l'Information et de la Communication

« Les TIC, technologies de l'information et de la communication, regroupent tous les outils, logiciels ou matériels de traitement et de transmission des informations : appareils photos numériques, téléviseurs, téléphones portables, ordinateurs, etc. D'une manière générale, tous les moyens de communication électronique sont visés, quelle que soient leur forme (écrite, imagée, parlée, etc.) et leur cible (clients, fournisseurs, entreprise, relations, etc.). Internet est un élément majeur des TIC, mais ce n'est pas le seul. » (Yolin, 2009)

Au travers des Technologies de l'Information et de la Communication, les entreprises peuvent poursuivre leur évolution digitale et donc utiliser des outils qui facilitent leur communication en interne mais aussi avec les parties externes à l'entreprise telles que les fournisseurs ou les clients.

Afin que le personnel dispose des outils adéquats pour travailler, deux entreprises belges sur trois donnent l'opportunité à leurs travailleurs de disposer d'appareils portables (ordinateur, tablettes, smartphone, etc.) qui les habilitent à avoir une connexion mobile à internet dans le cadre de leurs activités professionnelles (SPF Economie, 2016).

Les évolutions technologiques ont donné naissance à un nouveau mode d'envoi de factures. Bien que peu de personnes l'utilisent (comme nous le verrons dans le sous-point suivant), la dématérialisation des factures permet un traitement digital de ces dernières et représente un pas de plus vers la nouvelle ère digitale que connait notre époque.

4.2.1. La facture électronique (e-facture)

L'envoi de factures sous un format papier reste une pratique ancrée dans les mœurs de nos entreprises belges : 96,7 % des entreprises continuent à envoyer des factures papier. D'autres entreprises ont fait le pas et envoient des factures sous format électronique, toutefois 55,3 % des entreprises n'utilisent que le format papier (SPF Economie, 2016).

« En Belgique, une entreprise sur huit (12,3 %) envoie des e-factures permettant un traitement automatique et quatre entreprises sur dix (42,2 %) envoient des e-factures qui ne permettent pas de traitement automatique.

L'envoi de factures électroniques permettant un traitement automatique est une pratique nettement moins répandue dans les petites entreprises (9,6 %) que dans les grandes entreprises (45,3 %). » (SPF Economie, 2016, p. 46)

Tableau 2 : Pourcentage des entreprises envoyant des factures électroniques en fonction du format

(en %)	Entreprises	Grandes	Moyennes	Petites
Factures électroniques dans un format standard permettant leur traitement automatique	12,3	45,3	21,4	9,6
Factures sous forme électronique ne permettant pas de traitement automatique	42,2	61,2	47,4	40,6
Factures uniquement papier	55,3	30,5	48,9	57,2

Source : SPF Economie – DG Statistique – Statistics Belgium, Eurostat. (2015). *Enquête 'Utilisation des TIC et de l'e-commerce dans les entreprises'*. Récupéré de http://statbel.fgov.be/fr/binaries/Barometre_de_la_societe_de_l_information_2016_tcm326-278973.pdf, p. 41.

Au premier abord, ce que nous pouvons relever est que les petites et moyennes entreprises sont plus réticentes à l'utilisation de la facture électronique. De nombreuses petites structures ont un manque de confiance lié aux procédés électroniques, comme Eric Gryson (Chief Executif Officer de Ricoh Belgium SA) l'a souligné lors d'une interview en leurs bureaux : « Le véritable risque du digital est de ne pas être digitalisé ». Malgré cela, le changement peine à s'opérer mais devrait être un élément majeur que les sociétés devront prendre en compte dans les prochaines années.

4.2.2. La communication informatisée au sein des entreprises

Outre la facture électronique qui est une utilisation des moyens disponibilisés par les Technologies d'Information et de Communication, nous retrouvons également une capacité de communication améliorée au sein de la société par l'utilisation d'ERP.

« Un ERP est un logiciel de gestion qui va piloter l'activité de l'entreprise. Il a la particularité d'intégrer au sein d'une même base de données les principaux modules qui permettent de gérer l'activité d'une entreprise : gestion commerciale, gestion de la relation client, gestion financière, gestion de la production… ». (Axelor, 2017)

La communication au sein des entreprises est importante notamment entre les différents départements. Grâce au développement de progiciels ERP, une entreprise peut partager des flux d'information entre les différents départements qui la composent :

- Le département comptable ;
- Le secrétariat ;
- Le département des achats ;
- Le département des ventes ;
- Etc.

Dans notre plat pays, 50 % des entreprises utilise un ERP en 2015 contre 40,8 % en 2013 et 47,3 % en 2014. Il s'agit d'un outil est très utilisé par les grandes entreprises à hauteur de 88,9 % d'entre elles et les moyennes entreprises à hauteur de 74,2 % (SPF Economie, 2016).

Tableau 3 : Pourcentage des entreprises qui ont déjà utilisé un ERP

(en %)	Entreprises	Grandes	Moyennes	Petites
BE	50,0	88,9	74,2	44,5
UE 28	35,6	79,9	59,9	30,1
Max. UE 28	56,5	93,3	79,7	50,1

Source : SPF Economie – DG Statistique – Statistics Belgium, Eurostat. (2015). *Enquête 'Utilisation des TIC et de l'e-commerce dans les entreprises'*. Récupéré de http://statbel.fgov.be/fr/binaries/Barometre_de_la_societe_de_l_information_2016_tcm326-278973.pdf, p. 42.

5. La législation relative au numérique

Nous allons aborder la législation belge qui, selon Alexander de Croo, est en retard face au numérique. Si le numérique vient contraindre nos entreprises belges, la législation aussi doit pouvoir s'adapter et prévoir des mesures pour gérer au mieux le digital.

Selon un article paru en mars 2017 dans le journal L'Echo, la législation belge accuserait un retard important vis-à-vis du phénomène grandissant de la numérisation. Alexander de Croo, ministre de l'Agenda numérique, a déclaré que « la législation doit s'adapter à l'ère numérique ». Toutefois, la Cour d'Appel s'est opposée au « Digital Act » en déclarant que le caractère probant d'un contrat de vente qui aurait été conclu par e-mail ne pouvait pas être établi. (De Leus, 2017)

Nous aborderons également les dispositions du droit comptable relatives à la comptabilité informatisée. Nous analyserons celles-ci car dans la deuxième partie nous traiterons l'audit financier en milieu informatique, ce qui entraîne le respect de certaines règles quant à la conservation des documents sous forme électronique.

5.1. Digital Act[2]

Le 23 juillet 2014, l'Union Européenne adoptait un nouveau règlement européen[3] concernant l'identification électronique et les services de confiance que l'on appelle eIDAS. Ce règlement est entré en application le 1er juillet 2016 et vingt jours plus tard le législateur belge a adopté la loi du 21 juillet 2016 pour la mise en œuvre du règlement mais aussi pour le compléter de quelques dispositions afin de pouvoir créer un cadre juridique complet et harmonieux en matière d'archivage électronique.
La loi a été nommée « Digital Act » par Alexander de Croo et est entrée en vigueur le 28 septembre 2016. (Gobert, 2016)

Afin de mieux comprendre le règlement eIDAS, nous ferons état de son objectif principal. Ce règlement consiste à développer un cadre juridique afin de rassurer le marché intérieur grâce à une plus grande confiance dans les transactions électroniques. Le règlement reprend des dispositions en lien avec la signature électronique avec quelques modifications par rapport à la directive de 1999[4]. De plus, il ajoute de nouvelles dispositions quant à la reconnaissance (au niveau de l'Union européenne) de schémas d'identification électronique d'une part, mais d'autre part il complète cette directive de 1999 par des dispositions liées aux services dits de confiance qui sont additionnels à la signature électronique comme par exemple :

- Le cachet (qui prouve que le document est officiel) ;

[2] 21 juillet 2016. – Loi mettant en œuvre et complétant le règlement (UE) n° 910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, portant insertion du titre 2 dans le livre XII « Droit de l'économie électronique » du Code de droit économique et portant insertion des définitions propres au titre 2 du livre XII et des dispositions d'application de la loi propres au titre 2 du livre XII, dans les livres I, XV et XVII du Code de droit économique

[3] Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques

[4] Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques

- L'horodatage électronique (le fait d'ajouter une heure et une date à un document) ;
- Le service d'envoi recommandé électronique ;
- L'authentification de site Internet. (Gobert, 2016)

L'établissement des règles belges s'est fait dans le respect des objectifs et de la philosophie du règlement eIDAS. Ces règles comportent les mêmes principes que ceux que l'on retrouve dans le règlement européen pour les autres services de confiance tels que l'horodatage, les recommandés électroniques repris ci-dessus. Le but de ces règles est de couvrir aussi bien l'archivage électronique de documents qui ont déjà une source électronique ainsi que l'archivage électronique de documents papiers. (Gobert, 2016)

« Les dispositions envisagées cherchent manifestement à atteindre un équilibre entre souplesse et sécurité. D'une part, le législateur souhaite établir un cadre relativement souple pour stimuler l'offre des services d'archivage électronique, dans le respect des contraintes européennes, mais également leur utilisation aisée. D'autre part, ce cadre doit être suffisamment sécurisant pour protéger les utilisateurs de ces services et assurer un niveau minimum de qualité. » (Gobert, 2016, para. 8)

5.2. Dispositions comptables

Ce point fait état des différentes dispositions comptables relatives à l'utilisation d'un système informatique pour l'encodage de la comptabilité dans les sociétés. Pour ce faire, nous analyserons les avis de la Commission des Normes Comptables (CNC) qui reprennent les points sur lesquels nous devrons attirer notre attention lors d'une analyse de risques.

Les avis CNC que nous traiterons sont :

- L'avis CNC 2010/14 du 24 septembre 2010 portant sur la conservation des livres et des pièces justificatives.
- L'avis CNC 2016/22 du 28 septembre 2016 portant sur la conservation des livres et pièces justificatives en cas de tenue de comptabilité informatisée.

5.2.1. Avis CNC 2010/14 – Conservation des livres et des pièces justificatives

« En 2005, la tenue d'une comptabilité électronique a été légalement admis par la Loi comptable. En effet, l'article 2 de l'arrêté royal du 25 janvier 2005[5] érige en principe que les livres prévus par la loi peuvent tous être tenus soit sur support papier soit au moyen de systèmes informatisés. La comptabilité électronique devra, bien évidemment, répondre aux conditions et exigences imposées par la Loi comptable.

En ce qui concerne plus spécifiquement l'obligation de garantir la continuité matérielle, la régularité et l'irréversibilité (article 7, § 2 de la Loi comptable), l'article 5, § 2, de l'arrêté royal du 12 septembre 1983[6] prévoit que les systèmes informatisés utilisés (ex. logiciel comptable) doivent à tout le moins permettre à l'entreprise de tenir sa comptabilité conformément aux dispositions légales et réglementaires applicables à la tenue de la comptabilité. » (Commission des Normes Comptables, 2010, p. 1)

« Au regard de la législation TVA, les factures peuvent être transmises et reçues en Belgique par voie électronique sous réserve de l'acceptation du destinataire de la facture[7]. L'authenticité de l'origine et l'intégrité du contenu de la facture doivent en outre être garanties[8]. A compter du 1er janvier 2010, les entreprises belges ont la liberté de choisir la manière dont elles garantissent cette authenticité et cette intégrité10. Elles peuvent ainsi faire appel aux techniques informatiques (signature électroniques ou EDI) et opter pour d'autres solutions ou procédures, telles que le fait de lier la facture à un paiement, un bon de commande, un bon de livraison, etc. » (Commission des Normes Comptables, 2010, p. 2)

« L'article 9, alinéa 2 de l'arrêté royal du 12 septembre 1983 stipule explicitement, en matière de conservation des pièces comptables, que le support choisi doit assurer aussi bien

[5] Arrêté royal modifiant l'arrêté royal du 12 septembre 1983 portant exécution de la loi du 17 juillet 1975 relative à la comptabilité des entreprises, l'arrêté royal du 12 septembre 1983 déterminant la teneur et la présentation d'un plan comptable minimum normalisé et l'arrêté royal du 16 juin 1994 fixant la contribution des entreprises aux frais de fonctionnement de la Commission des Normes comptables, MB du 7 février 2005.
[6] Article 5, § 2 de l'arrêté royal du 12 septembre 1983 portant exécution de la loi du 17 juillet 1975 relative à la comptabilité des entreprises, introduit par l'article 2 de l'arrêté royal du 25 janvier 2005.
[7] Article 1er, § 2 de l'arrêté royal n° 1 du 29 décembre 1992 relatif aux mesures tendant à assurer le paiement de la taxe sur la valeur ajoutée.
[8] Article 60, § 3 du Code TVA.

l'inaltérabilité que l'accessibilité des données durant toute la durée de conservation. S'il s'agit d'une comptabilité électronique, cette obligation implique dans le chef de l'entreprise que cette dernière doit conserver non seulement les fichiers contenant les livres et les pièces justificatives, mais aussi les programmes et les systèmes qui permettent de les lire, et ce durant toute la période de conservation prescrite. En effet, chaque état comptable doit pouvoir être présenté et réimprimé pendant le délai de conservation minimum[9]. » (Commission des Normes Comptables, 2010, p. 2-3)

Le délai de conservation minimum a été ramené à sept ans. Il s'agit de sept ans à partir du 1er janvier de l'année suivant la clôture de l'exercice comptable.

5.2.2. Avis CNC 2016/22 – Conservation des livres et pièces justificatives en cas de tenue de comptabilité informatisée

« 14. Dans le cas d'une comptabilité informatisée se pose en effet la question de savoir ce que recouvre exactement l'obligation de conservation en original et dans le respect de l'inaltérabilité.
(…)
En pratique, en cas de comptabilisation informatisée, l'inaltérabilité suppose qu'il ne doit plus être possible de modifier, d'effacer ou d'ajouter des écritures.

Le respect de ces principes doit, par définition, être tout d'abord garanti en cours d'utilisation d'une solution informatisée de comptabilité avant d'envisager son respect à l'occasion de sa mise à jour ou d'un transfert de données vers la solution de destination en cas de changement de solution informatisée. » (Commission des Normes Comptables, 2016, p. 5-6)

En matière de « maintien des fichiers dans une version informatisée » nous sommes confrontés à deux possibilités : le maintien dans le même programme informatique ou l'archivage et le transfert de données vers un autre programme. Nous retiendrons que le plus important est que l'entreprise puisse assurer une continuité des activités. « Dans tous les cas de figure, la réalisation d'une sauvegarde (« back-up ») complète de la comptabilité sur une

[9] Article 9 de l'arrêté royal du 12 septembre 1983 portant exécution de la loi du 17 juillet 1975 relative à la comptabilité des entreprises.

base régulière participe à la bonne gestion de l'entreprise. » (Commission des Normes Comptables, 2016, p. 7)

« (…)
En conclusion, le maintien des fichiers informatiques dans une version rigoureusement identique pendant la durée légale de conservation de sept années n'est pas exigée à partir du moment où l'inaltérabilité, l'irréversibilité et la lisibilité des livres comptables et des données qu'ils contiennent, est garantie. » (Commission des Normes Comptables, 2016, p. 8)

Partie 2 : Contexte d'un audit financier en milieu informatique, notions, particularités et analyse de risques

Dans cette partie, nous adopterons le point de vue d'un auditeur qui est amené à réaliser ses travaux au sein d'une entreprise digitalisée. Le but est donc d'expliquer d'une part le travail d'auditeur en milieu informatique et quels points doivent attirer son attention et d'autre part de faire une analyse de risque afin de déterminer les différents risques auxquels les entreprises sont confrontées en adoptant le digital.

La mission d'un auditeur externe est de donner son opinion sur l'image fidèle et sincère des comptes annuels qui ont été établis par une entreprise. Deux options sont possibles :

- L'auditeur réalise des missions spéciales (comme lors d'un apport en nature, d'une acquisition, d'une fusion ou scission, etc.). Nous sommes alors dans le cas d'interventions contractuelles.
- L'auditeur certifie les comptes annuels et est commissaire aux comptes de l'entreprise.

Les activités de l'auditeur sont variées : il procède à l'identification des risques, il réalise une analyse des procédures de contrôle interne et donne une opinion positive ou négative sur l'image fidèle des comptes annuels des entreprises de tailles différentes, de la PME à la société cotée. (PWC, 2017)

Cette partie peut tout aussi bien s'appliquer au contrôleur interne qu'au contrôleur externe[10], la seule chose qui différenciera ces derniers est le degré d'indépendance vis-à-vis de l'entreprise auditée. Nous développerons essentiellement l'audit des systèmes informatiques qui nous intéresse plus particulièrement. Gardons toutefois à l'esprit que, même si l'entreprise est digitalisée, le travail d'un auditeur externe ne s'arrête pas seulement à la vérification des procédés liés à la digitalisation ! Il peut y réaliser des missions spéciales et certifier les comptes annuels.

[10] Sauf en cas de certification des comptes ou de missions spéciales

1. Identification des risques grâce à l'audit

Nous analyserons les différents risques connus lors de l'adoption d'une méthodologie de travail numérisée. La numérisation comporte différents risques auxquels les entreprises n'étaient pas confrontées lorsque les processus n'étaient pas informatisés, lorsque les différentes tâches ne dépendaient pas de l'intervention de la machine ou encore lorsque tous les documents étaient fournis en version papier.

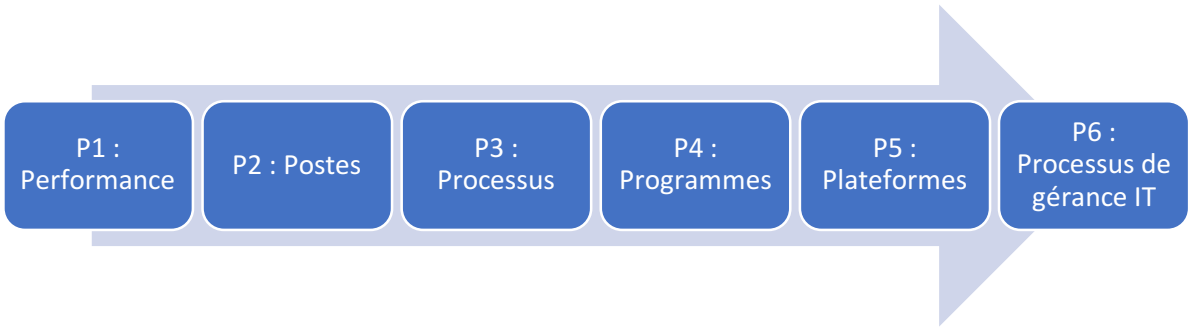
Nous tâcherons d'identifier la plupart des risques que nos petites et moyennes entreprises supportent en se digitalisant et ainsi pouvoir peut-être aider ces dernières à se préparer, à se prémunir d'outils afin d'entrer dans le processus digital sans être trop contraintes quant aux dangers relatifs.

Nous commencerons d'abord par les recommandations et le schéma d'audit mis en place par l'Institut des Réviseurs d'Entreprises permettant aux auditeurs de mener à bien leur audit en milieu informatique. Ensuite, lors de la troisième partie du mémoire, nous analyserons les risques que nous aurons relevés grâce à ce schéma.

Les risques que nous relèverons peuvent être mis en exergue par un auditeur si une entreprise le demande. Toutefois, le management de l'entreprise peut également faire sa propre analyse de risque. Lors de son analyse, l'auditeur peut pointer du doigt certains risques qu'il pourrait ne pas pouvoir « juger ». Prenons l'exemple d'un risque lié à un procédé informatique, l'auditeur seul (sans aide d'un expert informaticien) pourrait passer à côté du risque ou alors l'identifier mais sans pour autant pouvoir déterminer l'impact de celui-ci.

1.1. Recommandations de l'Institut des Réviseurs d'Entreprises

En matière de risques, l'Institut des Réviseurs d'Entreprises a établi un schéma de questions et de risques assimilés. L'IRE a mis en place des questions par paliers qui se présentent comme suit :



« **P1** :

- Quelle est la stratégie et la mission ?
- Quels sont les valeurs et objectifs clefs ?
- Comment les prestations sont-elles mesurées ? Quelle est la performance de l'organisation ?

P2 :

- Quels postes des comptes annuels sont importants ?

P3 :

- Par le biais de quels processus ces comptes annuels sont-ils établis ?
- Qui intervient au niveau des processus et quelles applications sont utilisées à cet effet ?

P4 :

- Quelles applications sont relevantes pour les processus importants et ont dès lors une influence directe sur les comptes annuels ?

P5 :

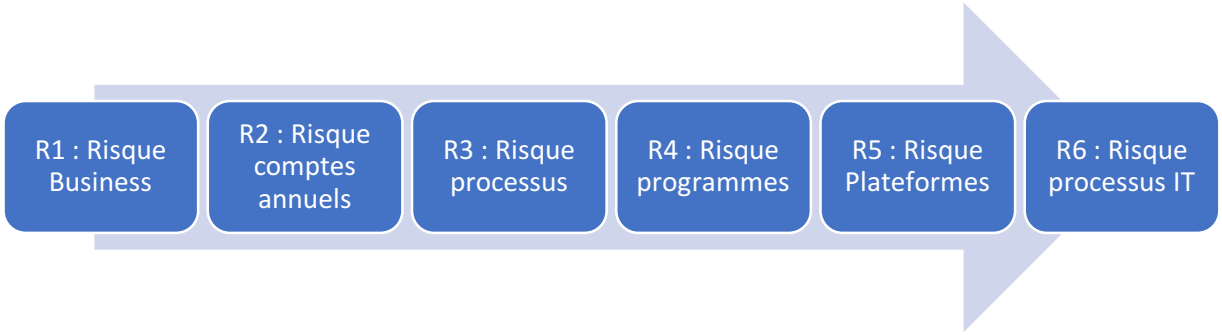
- Les applications fonctionnent sur quelles plateformes ?
- Quelles ressources sont utilisées par les applications ?

P6 :

- Quid continuité ?
- Quid changement de management ?
- Accès sécurisé ? » (icci, 2017, p. 8)

Nous avons pu donc voir quel type de questions un auditeur doit poser lors de ses travaux d'audit au sein d'une entreprise digitale. Il s'agit là d'un modèle établi par l'IRE dont le but est de donner un point de départ aux auditeurs pour favoriser leur audit financier dans un milieu informatique sans pour autant qu'ils aient des prédispositions en matière d'informatique (bien que celles-ci pourraient faciliter son travail).

Après avoir posé les différentes questions, nous pouvons procéder à l'analyse de risque et donc déterminer les différents risques en suivant le même schéma. L'IRE a donc détermine six risques établis en fonction du même modèle vu précédemment.



« **R1** :

- Quels risques de l'entreprise peuvent être reconnus ?

R2 :

- Quels risques ont une influence sur les comptes annuels (risque inhérent) ?

R3 :

- Quels sont les risques non-couverts par les processus (contrôle interne) ?

R4 :

- Quels sont les risques non-couverts par les applications ?

R5 :

- Quels sont les risques au niveau des plateformes ?

R6 :

- Quels sont les risques au niveau des processus de gérance IT ? » (icci, 2017, p. 12)

1.2. Détermination des risques

Nous pouvons définir plusieurs risques émanant de la numérisation. Ceux-ci sont liés aux activités de l'entreprise mais peuvent trouver leur origine dans différentes catégories que nous expliquerons par la suite. Nous considérerons l'organisation comme étant un « tout », nous

déterminerons donc les risques qui peuvent émaner des différentes parties prenantes d'une entreprise. Il peut s'agir de la direction, du personnel, des fournisseurs, du système informatique, etc.

1.2.1. Risques liés au système informatique

La digitalisation des procédés de l'entreprise suppose une rapidité croissante et donc à un gain de temps. Le but est donc de permettre à l'information de circuler plus facilement et plus rapidement et ceci permet la création de valeur. Cependant, nous remarquons que plus l'information est rapide moins on peut exercer un contrôle sur celle-ci. Face à cela, l'entreprise détermine le degré de contrôle qu'elle va exercer sur l'information dont elle dispose :

- Si la société applique un contrôle conséquent l'activité risque d'en pâtir et de subir un ralentissement important.
- Alors que si l'entreprise exerce un contrôle moindre, plus elle a de risques de subir des pertes d'informations. Le risque que l'entreprise encourt est donc de voir les données qu'elle détient être dérobées ou modifiées. (Cigref, 2011)

Les risques sont :

1. « Vol/altération/modification de données de l'entreprise par l'utilisation du système réseau par des employés.
2. Vol/altération/modification de données de l'entreprise par l'utilisation du système réseau par des pirates.
3. Vol/altération/modification de données de l'entreprise par l'utilisation du système réseau par des programmes malveillants (virus)
4. Déni de service entrainé par la saturation de réseaux ou des processus.
5. Ralentissement des activités. » (Cigref, 2011, p. 9-10)

Le premier risque auquel l'entreprise s'expose est le vol ou la modification de données détenues par l'entreprise et ce lors de l'utilisation du système informatique par les employés. Dans ce cas-ci, nous nous trouvons dans un cadre de malveillance interne. (Cigref, 2011)

Dans une telle situation, le travailleur dispose d'un accès à toutes les données sensibles que l'entreprise utilise dans le cadre de ses activités. Un employé qui est frustré par son travail ;

soit parce qu'il n'obtient pas ce qu'il désire de la part de son employeur, soit parce qu'il a décidé de nuire à l'entreprise dans son propre intérêt, peut faire usage de toute cette information en circulation à des fins malveillantes, ce qui peut s'avérer être très néfaste pour l'entreprise et la confiance qu'elle a obtenue de la part de ses clients.

Il est clair que plus l'employé a accès à des données importantes et hautement confidentielles plus la gravité du risque est importante. Les employés font partie intégrante de l'organisation et, dès lors, disposent d'informations sur l'entreprise et ses activités. Ceci fait que ce type de risque doit être traité consciencieusement par les dirigeants de l'entreprise.

Le deuxième risque supporté par l'entreprise est le même que le précédent mais cette fois-ci exercé par des hackers. Il ressort de l'étude réalisé par le CIGREF – un réseau français de grandes entreprises – que ce genre d'attaques subies par l'entreprise et exercées par des hackers étaient plutôt rares. Généralement, lorsqu'un hacker décide de s'en prendre à une entreprise c'est parce que ce dernier a une raison particulière pour le faire. (Cigref, 2011)

Bien que les médias nous inquiètent habituellement sur les piratages des entreprises par des hackers, le plus souvent les entreprises se voient être victimes d'actions « dommageables » de la part des employés internes à celles-ci. Par contre, il ne faut toutefois pas exclure l'éventualité d'une action entreprise par des hackers.

Prenons l'exemple d'Amazon Web Services (AWS), cette entreprise stocke de nombreuses données relatives à d'autres entreprises (par un service d'hébergement). Imaginons maintenant que AWS soit victime d'un piratage, de nombreuses entreprises utilisant ses services se verraient impactées et pourraient s'exposer à la perte de données extrêmement importantes à leurs activités ou encore pourraient subir un piratage des comptes bancaires. Récemment, le mardi 28 février 2017, AWS a subi une panne de cloud ce qui a impacté énormément de sites web. Le problème bien que fort dérangeant pour les entreprises ne fut pas gravissime en soi puisqu'il a pu être corrigé. Toutefois, pour de nombreuses entreprises le fait d'avoir une panne toute une journée peut engendrer une grande perte de recettes.

Le troisième risque est que l'entreprise subisse des dommages liés à des logiciels malveillants ou communément appelés « virus ». Bien que les entreprises soient exposées à ce genre de menace quotidiennement, la solution est assez primaire et les conséquences ne sont pas très

graves (Cigref, 2011). Généralement, toutes les entreprises disposent d'un antivirus qui leur permet de gérer les inconforts d'un virus. Toute entreprise utilisant des programmes informatiques et détenant des informations importantes sur les différents appareils, peut installer un antivirus afin de protéger et d'assurer le bon fonctionnement de ses outils.

Le quatrième risque est le déni de service qui provient de la saturation des réseaux ou des processus de l'entreprise. Lorsqu'une entreprise utilise le numérique, elle s'expose à saturer son réseau ce qui entraîne un amoindrissement de la production ou encore de la communication. Nous trouvons 2 sources quant au déni de service :

- Interne : comme par exemple le fait que le logiciel de facturation soit saturé par la quantité d'information.
- Externe : comme par exemple un problème technique avec un sous-traitant (AWS dont on parlait précédemment). (Cigref, 2011)

Le cinquième risque relevé est le ralentissement des activités de l'organisation. Ce ralentissement peut être lié à la pléthore de procédures mises en place pour contrôler tous les éventuels problèmes qui surgissent de la numérisation. Ce risque provient de la gestion du risque, ceci peut paraître confus mais est plutôt cohérent (Cigref, 2011). Comme présenté précédemment, deux choix s'offrent à l'entreprise ; soit elle accorde une haute importance au contrôle soit elle n'y accorde pas une si grande importance et n'intègre pas de lourdes procédures. Nous nous trouvons dans le cas où l'entreprise établi des procédures afin de contrôler toute l'information au maximum, ce qui entraîne que les activités de l'entreprise en pâtissent et se voient être ralenties. L'entreprise peut subir des pertes suite à ces ralentissements d'activité et de diminution de création de valeur.

1.2.2. Risques éthiques et juridiques

Les risques éthiques et juridiques regroupent essentiellement les risques qui sont liés à la confidentialité, au respect de la vie privée et l'authenticité des documents numériques. Nous retrouvons donc ici les risques suivants :

1. « Respect de la vie privée et confidentialité des données.
2. Internationalisation.
3. Authenticité des documents. » (Cigref, 2011, p. 8)

Le premier risque concerne le respect de la vie privée et la confidentialité des données dont l'entreprise dispose. Lorsqu'une entreprise décide de se digitaliser, elle procède à la numérisation des données confidentielles qui sont relatives à leurs clients ou à plusieurs collaborateurs. L'entreprise doit assurer la sécurité de toutes les informations qui auront été numérisées ! L'entreprise peut donc se retrouver dans des situations compliquées si elle ne sécurise pas les données, celle-ci peut faire face à des risques « juridiques » en cas de mauvaise protection des données. (Cigref, 2011)

L'entreprise est responsable de toute information concernant ses clients, elle doit en garantir la bonne conservation. Il ne faudrait pas que les clients se retournent contre l'entreprise et l'attaque en justice pour mauvaise utilisation d'informations confidentielles. Le plus grand défi des entreprises est certainement de conserver toutes ces informations contre toute attaque, que ce soit des attaques par des pirates ou par du personnel interne à l'entreprise.

Le deuxième risque concerne une notion un peu plus large, celle de l'internationalisation. Grâce à la digitalisation des entreprises, des informations les concernant peuvent se retrouver à l'étranger et les entreprises doivent prendre en considération les législations locales. Par exemple, comme nous le dit le Cigref, « les serveurs de données situés aux États-Unis sont soumis au Patriot Act, et la NSA a donc le droit de consulter les données qu'ils contiennent, ce qui présente un risque pour l'entreprise qui possède de tels serveurs (ou qui sous-traite l'hébergement de ses données à un fournisseur dont les serveurs sont situés sur le sol américain) » (Cigref, 2011, p.8).

Le troisième risque est lié à l'authenticité des documents. La légitimité des documents digitaux se voit être bien plus compliqué à prouver que le bien-fondé des documents en version papier. La production et la conservation des documents numériques entrainent plus d'obligations mais aussi plus de risques. Ces contraintes sont principalement en lien avec la gestion des documents. Prenons par exemple des documents comptables qui doivent suivre certaines dispositions techniques. (Cigref, 2011)

Afin de comprendre ce que représentent les « dispositions techniques », prenons l'exemple des factures qui sont établies entre un fournisseur et son client. Les factures sont établies selon un modèle où différentes informations doivent être communiquées. Chaque entreprise est

libre de les disposer comme elle le veut, toutefois les informations suivantes doivent être reprises (nous n'en citerons que quelques-unes) :

- La date de facture ;
- Un numéro séquentiel ;
- Le nom du fournisseur, son adresse et son numéro de TVA ;
- Mentions spéciales en cas de fournisseurs étranger (TVA intracommunautaire ou extracommunautaire) ;
- Le nom du client, son adresse et son numéro de TVA ;
- Le code TVA qui s'applique (IPCF, 2008)

  Outre les mentions habituelles de TVA nationale comme le 0 – 6 – 12 – 21 %, nous avons également deux mentions qui reviennent souvent :

  - Acquisition intracommunautaire[11]
  - Autoliquidation[12]

« Si ces données sont hébergées dans un autre pays, réparties sur différents sites (qui ne respectent peut-être pas les normes), ou non accessibles pendant un moment… en cas de contrôle fiscal, l'entreprise fait face à un risque juridique. » (Cigref, 2011, p. 9)

1.2.3. Risques liés à la gestion du personnel

Lorsqu'une entreprise décide de se digitaliser, le personnel peut s'en voir affecté. Les causes pourraient être liés au bouleversement des habitudes des membres de l'organisation, car évidemment le numérique entraîne de nouvelles procédures. De plus, qui dit digitalisation dit parfois licenciements. (Cigref, 2011)

Il n'est pas rare de voir que la digitalisation de certaines entreprises entraîne une restructuration au sein de celles-ci. Prenons le cas de la chaine de restaurant Kura – un restaurant japonais de sushis – qui s'est vu complètement automatisée. Nous prenons cet exemple car l'automatisation est une des formes de la digitalisation des entreprises. Kura est donc une chaine de restaurant automatisée, les consommateurs passent leur commande sur un

[11] En cas de livraisons visées à l'article 39bis, alinéa 1er, 4°, du Code TVA, (transferts assimilés à des livraisons intracommunautaires exemptées en Belgique).
[12] Lorsque le redevable est le cocontractant article 51, § 2, du Code TVA.

ordinateur. Il n'y a pas de serveurs et une fois les commandes enregistrées, les sushis défilent sur un tapis et les clients se servent. L'automatisation a permis à cette chaîne de restaurants de limiter les coûts de personnel et d'avoir un système rapide et efficace (Ford, 2015). Par contre, une des inquiétudes qui peuvent se poser est qu'un jour, et ce peut-être dans une avenir assez proche, l'élément humain d'une organisation ait disparu ou du moins soit drastiquement diminué.

Le Cigref a relevé trois risques qu'il définit comme étant majeurs :

- « Le manque d'adhésion ou le rejet par les employés de la politique de numérisation de l'entreprise ;
- Les risques sociaux ;
- La sclérose des compétences. » (Cigref, 2011, p. 7)

Il se peut que les employés d'une entreprise rejettent la nouvelle politique digitale de l'organisation. L'entreprise doit prévoir un éventuel rejet et mettre donc en place un encadrement pour opérer convenablement le changement vers le digital. Sans cet encadrement, la société pourrait se trouver face à un mécontentement et une réticence de la part des employés. Cette réticence peut se montrer sous différents aspects, par un malaise général jusqu'au rejet catégorique de l'outil digital. (Cigref, 2011)

Dans un cas pareil, nous nous trouverons à contre-courant des idées de création de valeur de la part de l'entreprise. Lorsque les membres du personnel sont défavorables à la politique digitale, l'entreprise ne peut en retirer un bénéfice ou avantage quelconque. De plus, procéder à des licenciements pourrait s'avérer très coûteux pour l'organisation. C'est pourquoi l'entreprise doit clairement définir une stratégie digitale qui prévoit un encadrement du personnel. Si l'entreprise ne prévoit pas un bon suivi de ses membres, cela pourrait engendrer un mouvement de déception et de rejet de la part des travailleurs.

Pour ce qui est des risques sociaux éventuels, l'entreprise doit prendre en considération le ressentiment des travailleurs en ce qui concerne la digitalisation de l'entreprise. Cette hostilité des employés peut prendre une forme collective et s'avérer donc être plus difficile à gérer pour la direction de l'organisation et son management. Dans le manque d'adhésion, le rejet de la part des employés ou encore dans la sclérose des compétences on peut se trouver avec quelques cas isolés alors que dans ce cas-ci on se trouve face à un ressenti général et

conséquent. L'entreprise peut se retrouver face à des différends avec la plupart des employés si la digitalisation a provoqué le licenciement de plusieurs travailleurs. L'entreprise pourrait voir sa productivité diminuer, ou pire encore être totalement à l'arrêt si jamais les employés procèdent à des manifestations. (Cigref, 2011)

Dans le milieu informatique et particulièrement dans le domaine des Technologies de l'Information et de la Communication, l'évolution digitale est très rapide. Il y a constamment de nouvelles technologies, et ainsi une nouvelle technologie peut rendre les compétences des employés obsolètes. Comme cette évolution est plutôt rapide, les entreprises optent parfois pour l'embauche de jeunes diplômés plutôt que de devoir prévoir des cessions de formation du personnel qui pourraient s'avérer plus couteuses puisque les diplômés auront déjà été drillés sur les nouveaux outils technologiques. (Cigref, 2011)

La numérisation des entreprises peut, en quelque sorte, mettre de côté les aspects sociaux d'un travail, c'est-à-dire que les entreprises cherchent à maximiser leur profit quitte à procéder à des licenciements. Le digital peut devenir le motif principal pour mettre au chômage toutes les personnes qui n'ont pas les compétences requises pour diriger les nouvelles technologies. Il y a là un problème d'ordre social que nous n'aborderons pas mais qui reste toutefois important ; si les entreprises ne forment plus les « seniors » qui n'ont pas connaissance des nouvelles technologies mais au contraire les licencient, qui va les engager à nouveau ? Il n'est pas impossible mais il est souvent compliqué pour des cadres d'entreprises ayant été licenciés de trouver du travail parce qu'ils sont plus chers que des jeunes diplômés. Ces anciens cadres devront peut-être alors se réorienter.

1.2.4. Risques stratégiques

Comme nous le présentions précédemment dans ce mémoire, lors de l'adoption du digital, l'entreprise doit penser à une stratégie dite digitale. Le but de la définition d'une stratégie digital est donc de pouvoir tirer profit, de pouvoir créer de la valeur par l'utilisation de la digitalisation. Toutefois, et comme toujours, ce n'est pas sans risque ! Nous pouvons définir des risques qui sont liés directement à la stratégie de l'entreprise face au numérique :

- « La défaillance de stratégie numérique ;
- Le lock in ;
- La concurrence entre deux supports de vente ». (Cigref, 2011, p. 10)

Le premier risque que nous avons défini est « la défaillance de stratégie numérique ». Celui-ci représente le plus grand risque lié à la définition d'une stratégie numérique. Il est risqué pour une entreprise d'avoir une stratégie digitale défaillante, voire de ne pas avoir de stratégie du tout ! Une entreprise doit se préparer convenablement à l'adoption de la stratégie digitale. Cependant, les décisions en termes de stratégie sont parfois mal déterminées par manque de connaissance vis-à-vis du numérique. Lorsque nous sommes en présence d'une défaillance de stratégie numérique, on peut se trouver face à des conflits internes au sein de l'entreprise comme par exemple une concurrence entre un poste numérique et un poste non numérique. Cette défaillance peut également amener à des pertes notamment si une entreprise digitalise des activités qui n'ont pas lieu d'être digitalisées. Développer les systèmes en interne est plus long pour l'entreprise alors que des solutions externes sont prêtes à être utilisées. (Cigref, 2011)

Pour ce qui est du lock in, « il s'agit de la situation dans laquelle une entreprise est dépendante d'un fournisseur et ne peut passer à la concurrence que pour un coût prohibitif » (Cigref, 2011, p. 10). Il s'agit d'un phénomène que l'on retrouve le plus souvent dans le monde informatique. « Être enfermé peut empêcher l'interopérabilité des systèmes en interne et en externe, mais aussi entrainer une incapacité à évoluer qui entraine une perte de l'avantage concurrentiel, finalement un manque à gagner voire une perte. » (Cigref, 2011, p. 10)

Le lock in est fort présent dans les entreprises qui travaillent sur cloud. Par exemple, Excellium Solution – l'entreprise pour laquelle nous ferons une analyse de risque – utilise le cloud auprès d'un sous-traitant, si ce dernier connait une panne l'entreprise de comptabilité ne pourra pas continuer son travail. Le lock in fait que la fiduciaire est dépendante de son sous-traitant cloud et qu'elle ne peut envisager de changer de fournisseur sans devoir supporter des coûts importants.

Le dernier risque lié à la stratégie est la concurrence entre deux supports de vente. Dans ce cas-ci, nous nous trouvons dans la situation où la digitalisation de l'entreprise est en lien avec sa capacité de vente, comme par exemple la création d'une plateforme internet de vente en ligne. À partir du moment où l'entreprise a mal planifié sa stratégie digitale ou bien que le marché cible de l'entreprise a eu un engouement important pour le site internet, elle peut se trouver face à la « cannibalisation » c'est-à-dire qu'à l'instar de gagner des clients, les mêmes

clients seront partagés sur les deux points de vente (en ligne et en magasin). Ce qui peut être un peu plus grave, c'est que la clientèle cesse d'aller en magasin et ne passe plus que par la plateforme internet. (Cigref, 2011)

1.2.5. Risques marketing

Le secteur marketing connait des risques liés à la digitalisation qui sont préjudiciables au niveau de la réputation de l'entreprise mais aussi au niveau de sa performance en termes de ventes auprès des clients. (Cigref, 2011)

La réputation de l'entreprise est extrêmement importante. Les outils de communication et de marketing tels que des sites internet sont des outils fragiles et fort vulnérables. Ce type d'outils se confronte parfois à des attaques de la part de personnes malintentionnées vis-à-vis de l'entreprise. L'entreprise est face à un réel risque en termes d'image. Peu importe qu'il s'agisse d'une campagne organisée ou de mécontentements tangibles, en offrant un espace « libre » en plein cœur de son instrument de communication l'entreprise encoure un risque accru d'attaques qui nuisent à leur réputation. (Cigref, 2011)

L'entreprise voit également sa concurrence être accrue et plus présente. La capacité d'une entreprise à vendre sur des plateformes en ligne peut être améliorée, voir même connaître ses débuts pour certaines entreprises. Cependant, une plateforme en ligne est contrainte aux mêmes conditions qu'un point de vente « physique » et l'entreprise peut se trouver face à une concurrence ardue sur un « marché en ligne ». Toutefois, le pouvoir de la concurrence ou l'ampleur de celle-ci est décuplée du fait que le marché de l'internet ne connait pas de frontières contrairement à un point de vente physique qui lui est confronté à une concurrence localisée. Nous assistons également depuis quelques années au développement de comparateurs de prix qui augmentent le degré de compétitivité que l'entreprise doit avoir. La concurrence est étendue et plus forte. (Cigref, 2011)

1.2.6. Risques en lien avec la dématérialisation des relations humaines

Lorsqu'une entreprise passe au digital, cela entraîne une dématérialisation des rapports humains qui engendre une perte de communication « physique » entre les individus. Nous pouvons retrouver cette dématérialisation tant entre personnel mais également entre des

membres de l'organisation et des parties externes telles que les clients et les fournisseurs. (Cigref, 2011)

Nous retrouvons dans cette dématérialisation des relations humaines des risques tels que :

- « L'affaiblissement de la communication ;
- La perte de souplesse ;
- La perte du temps de réflexion ;
- L'infobésité. » (Cigref, 2011, p. 11-12)

Lorsque nous parlons d'affaiblissement de la communication nous faisons allusion à la mutation des relations sociales qui entraînent une transformation de la communication. Les moyens actuels de communication sont plus performants et plus nombreux. Toutefois, nous remarquons qu'il existe quand même un penchant à moins communiquer. Par ailleurs la qualité de la communication peut, elle-aussi, être sujet à un amoindrissement et c'est ce point qui doit être analysé attentivement par les entreprises. Ce phénomène porte un nom : le Paradoxe de Maslow. Il existe moins d'interactions entre les membres du personnel car les moments que nous connaissions comme les discussions autour de la machine à café ou encore les discussions directes se font moins présentes voire même sont en voie de disparition. (Cigref, 2011)

La digitalisation des procédés de l'organisation tend généralement vers la simplification des procédures de décision, particulièrement dans le secteur bancaire. Ce qui est contraignant est que cela se fait parfois au détriment d'étapes clefs de discussions et d'échanges ; que ce soit avec les fournisseurs, les clients ou encore les employés de l'organisation. Bien que cela soit favorable pour l'entreprise en termes de gain de temps, l'entreprise se soumet également à une perte de souplesse et en capacité d'adaptation ce qui amène l'entreprise à devenir beaucoup trop raide face à une concurrence parfois plus flexible. (Cigref, 2011)

En matière de réflexion, les acteurs économiques tels que les clients, les fournisseurs, les entreprises, les employés, les dirigeants sont contraints à une perte de temps due à l'accélération de l'économie et des échanges issus de la digitalisation de l'information. Ceci leur laisse moins de temps pour penser et se positionner. Le risque que nous pouvons identifier pour les entreprises est que ces dernières se retrouvent dans une situation où elles n'ont plus l'aptitude d'anticiper le marché. (Cigref, 2011)

L'infobésité est un phénomène assez connu. Ce phénomène renvoie à l'excès d'information digitale présente chaque jour et sous différentes formes. Une communication efficace demande l'emploi de plusieurs canaux. Cependant, la dématérialisation des relations humaines amène un accroissement net du volume d'information digitale traitée par les travailleurs au sein de l'entreprise. L'organisation risque de voir ses canaux de communication saturés et une partie de toute l'information disponible sera perdue ou mal traitée. (Cigref, 2011)

1.2.7. Risques en lien avec le patrimoine digital

Cette catégorie de risques est composée des risques qui sont en lien avec la conservation de données sous forme digitale ; que ce soit notamment le vieillissement des supports ou encore l'évolution des formats. Dans cette catégorie, nous retrouvons également les risques liés à la valorisation financière fort compliquée du patrimoine digital mais aussi les risques attachés aux garanties des produits digitaux. (Cigref, 2011)

Nous avons vu précédemment que lorsque l'entreprise conservait des données sous format digital, elle pouvait s'exposer à des risques juridiques. Lorsque cette dernière faisait état d'une mauvaise conservation des données, elle pouvait encourir des pertes. « La durabilité des supports et des formats n'est pas facile à assurer dans le cadre du stockage numérique » (Cigref, 2011, p. 12). De plus, les entreprises sont souvent amenées à sous-traiter l'hébergement des différentes données numériques dont elles disposent, ce qui fait que le contrôle sur les moyens de protection et de conservation ne peut être correctement assuré par l'entreprise et l'accès à l'information peut être momentanément restreint. Pour finir, nous ne devons pas mettre de côté les risques possibles liés à des éventuelles catastrophes naturelles que pourraient subir les datacenters en cas de cloud computing ce qui nuirait gravement aux entreprises en stoppant ou ralentissant leur activité. (Cigref, 2011)

Nous verrons par la suite que les catastrophes naturelles sont moins dangereuses que nous le pensons. Les datacenters sont généralement nombreux ce qui permet de conserver des copies des données au cas un datacenter subirait un dommage quelconque qui pourrait entrainer la perte totale de données. Ceci nous amène à croire que ce risque éventuel lié à une catastrophe naturelle est contrôlé. Nous y reviendrons dans l'analyse de risques faite au sein d'Excellium Solution.

« Valorisation financière. Les méthodes pour calculer la valeur d'une entreprise sont mal adaptées au calcul de la valeur d'une entreprise 100 % numérique. En effet, celle-ci ne dispose pas d'actifs réels mais immatériels, dont la valorisation est difficile. La valeur de l'entreprise numérique peut donc être mal évaluée par les institutions financières, ce qui a des conséquences au niveau de ses actionnaires et investisseurs. Par ailleurs, la sous-évaluation de l'entreprise numérique peut entraîner des difficultés vis-à-vis des institutions bancaires, qui peuvent refuser de la financer, ce qui peut provoquer un risque important pour la poursuite des activités ou le développement de l'entreprise. » (Cigref, 2011, p. 12)

La valorisation des avoirs « immatériels » de l'entreprise peut être compliquée. Les avis divergent sur le fait qu'une entreprise 100 % numérique dispose ou non d'actifs réels. Cela peut nous amener à penser que l'entreprise n'a pas d'actif physique parce qu'elle est 100 % digitale, ce qui est faux dans la plupart des cas ! Pour plus qu'une entreprise soit digitale, elle aura toujours besoin d'outils physiques pour diriger son activité numérique ; que ce soit des ordinateurs, smartphones ou autres appareils électroniques.

Cette phrase pourrait être vraie dans la mesure où une entreprise sous-traite toute la gestion de l'activité à des sous-traitants, et encore il n'est pas sûr que l'entreprise ne détienne pas des immobilisations corporelles.

Pour ce qui est des produits numériques non garantis (comme par exemple la batterie d'un ordinateur), nous pouvons relever un risque pour l'entreprise. La garantie de tels produits n'est pas toujours aussi bien définie que lorsqu'il s'agit de produits matériels que nous connaissons bien et cela entraine un risque supplémentaire pour les entreprises. Un problème quelconque résultant de l'utilisation de produits pour lesquels il n'y a pas de garanties engendre des conséquences que les entreprises devront gérer d'elles-mêmes puisqu'elles ne disposeront pas de base légale pour se retourner contre les producteurs. L'entreprise est donc contrainte à assumer le risque lié à l'utilisation de produits digitaux. (Cigref, 2011)

1.2.8. Risques périphériques

Nous nous trouvons ici dans la dernière catégorie de risques identifiés par le Cigref. Cette catégorie répertorie les risques qui sont liés à une perte de contrôle des produits ou encore de

la situation géopolitique. Ces derniers paraissent être plutôt exceptionnels mais ne sont pas moins dangereux pour l'entreprise. (Cigref, 2011)

Le Cigref nous rapporte que depuis l'entame des années 80 et depuis l'apparition de l'informatique – voire même du numérique de nos jours – une part de l'économie s'est retrouvée dématérialisée. En moins de quinze ans, les flux financiers et d'informations ont connu un accroissement considérable. La dématérialisation desdits flux nous a démontré par le passé que les impacts des risques connus ont largement été diminués. La digitalisation a fait en sorte que tous les flux soient amplifiés et accélérés, ce qui a provoqué la perte de contrôle sur ceux-ci. (Cigref, 2011)

« C'est ainsi que nous avons vu se développer la crise des pays asiatiques, la quasi faillite de l'Angleterre (due à la spéculation du fond d'investissement de Soros), la crise des subprimes (les banques ne sachant plus dans un premier temps si elles possédaient ou non des Crédit Default Swap). Tous ces événements sont symptomatiques des risques périphériques à l'entreprise (et parfois à l'État) dont les impacts sociaux et économiques ne sont peut-être pas identifiables en amont mais dont les conséquences peuvent être dévastatrices. La numérisation de l'entreprise implique une refonte des pratiques de bonne gouvernance. » (Cigref, 2011, p. 13)

L'entreprise se retrouve face à des outils dont elle n'a pas toujours le contrôle. Nous pouvons prendre l'exemple d'une entreprise travaillant sur le Cloud. Cette entreprise ne détient pas le contrôle absolu sur l'outil principal de son environnement de travail. Comme nous le citions précédemment, l'activité peut se voir être arrêtée momentanément car l'entreprise dépend d'un outil géré par un sous-traitant.

Nous pourrions être amenés à croire dans un premier temps qu'une entreprise digitale se défait du « risque pays », toutefois celui-ci est encore bien présent de nos jours bien que sous d'autres formes grâce au numérique. « On peut citer l'exemple du Myanmar, où des attaques de DDoS (attaques par déni de service -denial of service attack) ont isolé le pays du réseau internet pendant les sept jours précédant les premières élections politiques en 20 ans (et où l'origine politique de cet acte peut être suspectée). » (Cigref, 2011, p. 13)

2. Notions sur l'audit des systèmes informatiques

Dans ce chapitre nous ferons le point sur les différentes notions de base afin d'avoir une meilleure compréhension globale sur l'audit en milieu informatisé en abordant les différentes composantes du métier. Nous disposerons ainsi des notions de base afin d'aborder la suite du travail.

2.1. Les concepts de base pour comprendre l'audit des systèmes informatiques (SI)

« Un système informatique est un ensemble des moyens informatiques et de télécommunication ayant pour finalité d'élaborer, traiter, stocker, acheminer, présenter ou détruire des données. Le système informatique est la partie informatique du système d'information, composée de matériels, logiciels, réseaux et procédures d'utilisation. » (Marché Public, 2013)

Le but de ce type d'audit est d'évaluer les risques d'un environnement informatique mais aussi d'une application, un logiciel comme SAP par exemple. Afin de réaliser les missions, l'auditeur choisira avec le client les différents processus à évaluer. (ICCI, 2017)

La raison d'un tel audit peut être lié à l'évaluation de plusieurs risques informatiques liés à la sécurité logique et physique, mais aussi à l'administration des changements ou encore du plan de secours. Cet audit peut également concerner un ensemble de processus informatiques mis en place afin de répondre à des demandes particulières venant des clients. (ICCI, 2017)

2.2. Phases d'audit informatique

Un audit informatique, un audit des Systèmes Informatiques comporte :

1. « Définition précise du plan de travail, récolte d'information, recherche et schématisation des processus métiers et/ou informatiques à apprécier, définition des rôles et responsabilités, analyse des forces-faiblesses.
2. Analyse des processus importants, définition des risques, évaluation préliminaire des risques, de l'efficacité des contrôles.
3. Tests des contrôles.
4. Tests de matérialité. » (ICCI, 2017, slide 26)

L'auditeur doit prendre connaissance de l'environnement dans lequel il se trouve puisque bien évidemment toutes les entreprises ont leurs propres caractéristiques, il s'agit de la définition du plan de travail et de la récolte d'information. Ceux-ci sont définis lors d'un audit intérimaire. Il s'agit d'un audit que l'on opère en milieu d'exercice afin de faire une situation intermédiaire pour prendre connaissance des processus de l'entreprise ou des nouvelles acquisitions qui peuvent être informatiques ou de tout autre ordre.

Lors de l'analyse des différents processus clefs de l'entreprise, nous devrons relever les différents risques que l'entreprise supporte en utilisant l'un ou l'autre processus. Des risques tels que la perte de données, les virus amenés par des logiciels malveillants, le hacking, etc.
Le but est d'aider l'entreprise à détecter les risques mais aussi de pointer quels sont les processus les plus à risques et ceux qui le sont moins.

En fonction de ce qui est testé dans l'entreprise, en fonction des différents postes du bilan, les contrôles seront différents. Par exemple, lors d'un audit de fin d'exercice, l'auditeur va analyser le poste 490 – Charges à reporter. Lors de cette analyse, l'auditeur vérifiera que l'entreprise a bien comptabilisé toutes les charges correspondantes à l'exercice suivant dans ce compte.

Les contrôles sont généralement déterminés en fonction d'un seuil de matérialité. L'auditeur détermine un seuil (de matérialité) en dessous duquel il accepte un degré d'erreurs. Tout poste du bilan qui soit supérieur à ce seuil fera l'objet de contrôle afin de détecter une quelconque anomalie. Le seuil de matérialité est déterminé en fonction de l'analyse de risque. Suite à cette analyse, l'auditeur déterminera le seuil de signification :
Il appliquera par exemple 5 % du bénéfice avant impôt s'il s'agit d'une entreprise avec but lucratif, tandis que pour une entreprise sans but lucratif il appliquera 1 % du chiffre d'affaires ou des recettes.

2.3. Les différents types d'audit en milieu informatique

2.3.1. Audit de l'infrastructure informatique

L'objectif d'un tel audit est de pouvoir évaluer les différents risques émanant des systèmes d'information qui sont nécessaires au bon fonctionnement des applications. Comme les

risques que nous déterminions plus tôt dans le point 1.1, à savoir : la sécurité physique et logique, ou encore le plan de secours ou encore d'autres risques comme la sécurité des réseaux par exemple.
Dès lors, un rapport qui comprend les faiblesses qui ont été relevées, le niveau de risque relatif à ces faiblesses et les dispositions rectificatives qui sont proposées, sera établi. (ICCI, 2017)

2.3.2. Audit d'une application en cours d'exécution

L'audit d'une application informatique qui est en cours d'exécution est réalisé dans le but de soutenir l'équipe de projet dans l'évaluation des risques tout au long des différentes étapes d'exécution d'une application informatique. Le but est de promouvoir des mesures dans l'optique de réduire et de contrôler les risques majeurs et de vérifier également la force des processus de gestion des changements du nouveau système d'information. (ICCI, 2017)
« On distingue les contrôles applicatifs suivants :

- Création et autorisation ;
- Saisie et enregistrement des données ;
- Traitement des données ;
- Sortie des données (output) ;
- Interfaces.

L'objectif des contrôles applicatifs est d'assurer que :

- Toutes les données inputs sont exactes, complètes, autorisées et correctes ;
- Toutes les données sont traitées comme convenu dans une période acceptable ;
- L'enregistrement des données est exact et complet ;
- Les outputs sont exacts et complets ;
- Un enregistrement est maintenu pour tracer le traitement des données depuis l'input jusqu'à l'enregistrement et à l'output éventuel. » (ICCI, 2017, slides 28 - 29)

L'output de cet audit consiste en des mesures visant à réduire et contrôler des risques importants de la nouvelle application informatique.

Un exemple tout simple serait de modifier régulièrement les mots de passe des applications. De plus, un mot de passe est plus difficile à trouver lorsqu'il a plus de 10 caractères. Ne

pensez pas qu'un code de 6 digits avec majuscules, minuscules et chiffres est fiable ! En termes de mots de passe, plus ils sont longs moins ils sont sujet à un piratage « facile ».

2.3.3. Audit d'une application informatique

Lors de la réalisation de ce type d'audit, l'objectif est de comprendre une application informatique en fonctionnement, comme une application financière par exemple, ou encore une application de gestion des salaires, etc. La plupart du temps de nombreux domaines font partie intégrante de l'audit d'une application, particulièrement :

- « Les données opérationnelles ;
- Les données de base ;
- Les paramètres ;
- Les interfaces entre l'application et d'autres applications ;
- La gestion des droits d'accès à l'application. » (ICCI, 2017, slide 30)

Il est évident que tout audit lié à une application doit aussi évaluer la sécurité relative à l'infrastructure informatique qui est indispensable au fonctionnement de l'application. Nous nous baserons également sur un rapport qui reprend les différentes faiblesses qui ont été relevées suite à l'audit, le niveau de risque qui est lié aux faiblesses et des propositions de mesures correctrices. (ICCI, 2017)

2.3.4. Missions spécifiques

L'auditeur est parfois confronté à des missions spécifiques telles que :

- « La maîtrise des coûts informatiques
- L'audit de la politique informatique
- L'audit sécurité (cf. audit de la sécurité informatique)
- L'audit du respect de la vie privée » (ICCI, 2017, slide 31)

La maîtrise des coûts informatiques

Il s'agit d'un audit informatique qui aide une entreprise à améliorer ses outils selon différents critères comme :

- Le degré d'intégration de l'informatique dans l'entreprise ;

- La planification de l'évolution de tous ces outils ;
- L'optimisation des compétences informatiques.

L'audit de la politique informatique

Cette mission consiste en l'analyse de la politique (stratégie) mise en place au niveau informatique, on peut le lier à l'audit de sécurité puisque la sécurité informatique représente une partie de la stratégie informatique.

2.4. Les classifications des contrôles d'audit

Les contrôles d'audit peuvent être classés en fonction de différentes catégories :

- Preventive / Detective / Corrective
    - **Audit préventif** : Un contrôle est effectué avant que des erreurs ou que des problèmes ne surgissent.
    - **Audit de détection** : Le problème est survenu, nous allons chercher à en trouver la source.
    - **Audit correctif** : Nous tenterons de corriger un problème rencontré.
- Generale & Application
    - Les contrôles d'application visent à contrôler les systèmes informatiques de l'entreprise (applications telles que Navision, SAP, etc.).
- Administrative & Comptable
- Entrée – Traitement – Sortie
    - Ceux-ci font partie des contrôles applicatifs. Pour le contrôle des entrées par exemple : le but est de vérifier l'intégrité des données introduites.

3. Le pilotage d'un audit en milieu informatique

Le but du concept d'audit informatique est de pouvoir évaluer la mise en règle des processus (que ceux-ci soient conformes) et méthodes de l'entité avec un nombre de règles en vigueur ; des règles d'ordre juridique, fiscal ou encore technologique, etc.

À partir du moment où la société prend la décision – ou est obligée (dans le cas où elle a un commissaire aux comptes) – de réaliser un audit, elle va être amenée à réfléchir sur la manière de mener à bien cet audit et se posera également des questions afin de pouvoir appréhender

avec un maximum d'objectivité les différents résultats des diverses investigations qui auront été réalisées. (ICCI, 2017)

Afin de bien se préparer à l'audit de son système informatique, une entreprise doit garder à l'esprit les éléments suivants :

A. « Bien délimiter les champs d'investigation et les enjeux de l'audit ;
B. Se préparer à la procédure d'audit ;
C. Séparer le commanditaire de l'entité en charge de l'audit ;
D. Se doter d'une direction de l'audit ;
E. Recourir à des référentiels solides ;
F. S'entendre sur le référentiel choisi ;
G. Préparer les pièces indispensables à l'audit et en faciliter l'accès ;
H. Confier son audit à une équipe pluridisciplinaire et indépendante ;
I. Choisir la fréquence et le temps de déroulement de l'audit ;
J. Ne pas sous-estimer les limites d'un audit. » (ICCI, 2017, slides 37 à 46)

3.1. Bien délimiter les champs d'investigation et les enjeux de l'audit

L'audit des Systèmes Informatiques couvre de nombreux domaines et qui peuvent être complètement opposés. On peut y retrouver les domaines suivants :

- Les processus ;
- La sécurité du Système Informatique, par exemple les mots de passe ou encore les systèmes de backup ;
- La gestion des droits d'accès, par exemple la création de nouveaux accès utilisateurs avec délimitation des pouvoirs.

Il existe donc une vaste typologie d'audits qui peut être répartie en deux groupes : l'activité informatique et les applications additionnées des processus métier.
L'audit de l'activité informatique peut comprendre l'audit de la stratégie digitale – que nous évoquions plus tôt dans la première partie – mais aussi l'audit de l'opérationnel ou encore du management de la fonction informatique. Alors que l'audit des applications comprendra différentes activités particulières comme par exemple dans le cas de la gestion commerciale la validation de données, la fiabilité, la conformité des règles, etc. (ICCI, 2017)

Une entreprise doit donc s'assurer de la force de sa stratégie informatique et donc vérifier les processus mis en place en matière de protection des données avec des systèmes de backup par exemple. D'autre part, il faut également s'assurer de la fiabilité des applications, soit des différents outils informatiques dont l'entreprise dispose et que ceux-ci fonctionnent de manière fiable et avec le moins d'erreurs possible.

3.2. Se préparer à la procédure d'audit

L'entreprise doit s'assurer de pouvoir mieux identifier les différents points qui lui posent problème, ce qui la rend vulnérable. La société doit d'abord se conscientiser du fait qu'elle a des lacunes propres et doit également prendre des mesures afin de déterminer la raison, le pourquoi, de ces lacunes. Ainsi, elle pourra penser à améliorer et confronter les procédures défaillantes existantes. (ICCI, 2017)

La procédure d'audit va donc permettre à l'entreprise, d'une part, de découvrir une possible menace vis-à-vis de laquelle elle n'a pas pris le temps de se préparer. D'autre part, l'administration pourra également souligner une supposition de vulnérabilité de par la procédure d'audit. (ICCI, 2017)
Il est important de relever qu'il existe deux types d'audit :

- Les audits planifiés
- Les audits opérés à chaud

Les audits planifiés sont ceux qui se passent comme prévus, ceux qui ont été préparés à être réalisés au sein de l'entreprise.

Ceux réalisés à chaud seront mis en place lorsque l'audit ne se passe pas comme prévu, ou quand la société se trouve dans une situation de conflit avec un fournisseur qui ne permet pas le bon déroulement de l'audit prévu initialement par exemple. (ICCI, 2017)

3.3. Séparer le commanditaire de l'entité en charge de l'audit

L'auditeur ne doit pas se laisser influencer par l'autorité de la personne qui demande la réalisation de l'audit. On parle alors de scepticisme de la part de l'auditeur qui se fera sa

propre opinion sur les comptes et les processus qu'il analyse tout en tenant compte de ce qui lui est rapporté par la direction.

3.4. Se doter d'une direction de l'audit

Il n'y a que les plus grandes organisations qui peuvent se permettre de mobiliser des capacités internes suffisantes et adéquates afin de créer une cellule qui se dédiera à l'audit. Cependant, cette structure ne peut être viable économiquement uniquement de par son rattachement à la Direction des Systèmes d'Information (DSI). Il faut que cette cellule soit également rattachée à un niveau décisionnel plus important et ne pas uniquement être liée à la DSI. (ICCI, 2017)

La Direction des Systèmes d'Information ne doit pas seulement être là pour diriger les différents systèmes d'exploitation informatiques de par sa connaissance en la matière, elle n'est pas cantonnée qu'à cette fonction. Elle doit également anticiper l'évolution de facteurs externes comme l'évolution de la stratégie de l'entreprise et participer, elle-aussi, aux décisions prises par l'entreprise.

3.5. Recourir à des référentiels solides

Nous connaissons différents référentiels utilisés actuellement comme :

- « ISO ;
- COBIT – Control Objectives for Business and related Technology ;
- CMMI – Capability Maturity Model Integration ;
- ITIL – Information Technology Infrastructure Library. » (ICCI, 2017, slide 41)

Les normes ISO constituent des normes internationales qui fournissent des règles ou qui représentent une ligne directrice relative à une activité particulière afin de déterminer le « degré optimal d'ordre dans un contexte donné ». Nous les retrouvons sous de nombreuses formes comme par exemple : des normes de produits ou des formules d'essai ou encore des codes de bonne pratique, lignes directrices et normes de systèmes de management. (ISO, sd)

Le référentiel COBIT est celui développé par l'Information Systems Audit and Control Association (ISACA). Ce dernier décompose les différents systèmes informatiques utilisés dans les entreprises en quatre catégories :

- Planification et organisation :

  « Couvre la stratégie et les tactiques et concerne l'identification des moyens permettant à l'informatique de contribuer le plus efficacement à la réalisation des objectifs commerciaux de l'entreprise. » (Aud-IT, 2012, para. 2)
- Acquisition et installation :

  « Concerne la réalisation de la stratégie informatique, l'identification, l'acquisition, le développement et l'installation des solutions informatiques et leur intégration dans les processus commerciaux. » (Aud-IT, 2012, para. 3)
- Livraison et support :

  « Concerne la livraison des prestations informatiques exigées, ce qui comprend l'exploitation, la sécurité, les plans d'urgence et la formation. » (Aud-IT, 2012, para. 4)
- Monitoring.

  « Permet au management d'évaluer la qualité et la conformité des processus informatiques aux exigences de contrôle. » (Aud-IT, 2012, para. 5)

Les deux autres sont également des référentiels dont le but est aussi de permettre un degré d'ordre parmi les différentes activités.

3.6. S'entendre sur le référentiel choisi

Il faut que toutes les parties concernées par l'audit, que ce soit l'auditeur ou l'administration ou encore les personnes qui prennent part à l'audit, soient mis au courant et aient une vision sur le référentiel qui est choisi. Ainsi, cette mise en conformité va s'assurer de la clarification de la démarche d'audit. (ICCI, 2017)

3.7. Préparer les pièces indispensables à l'audit et en faciliter l'accès

Il y a une pièce qui est essentielle pour réaliser un audit des Systèmes d'Information : Le cahier des charges. Celui-ci a pour but de mettre sur papier et de rendre contractuel les besoins d'une entité vis-à-vis de personnes tierces. Il ne s'agit cependant pas de l'unique document nécessaire lors de la réalisation de l'audit, nous retrouvons également :

- Le plan qualité ;

- Les tableaux de bord (outil de gestion fort utile qui présente les activités et les résultats de l'entreprise par processus) ;
- Les KPI's (Key Performance Indicators – ceux-ci doivent permettre à l'entreprise de mesurer le progrès réalisé ou encore à réaliser). (ICCI, 2017)

Les indicateurs clefs de performance peuvent être les suivants :

- Délai moyen de paiement client
- Délai moyen de paiement fournisseur
- Temps passé sur le site
- Nombre d'heures supplémentaires

3.8. Confier son audit à une équipe pluridisciplinaire et indépendante

Un audit ne se réalise pas tout seul, ce travail repose sur les différentes ressources humaines qui sont mobilisées pour son parachèvement. Il faut que les personnes attelées à la réalisation de l'audit soient dotées de compétences propres à chacun afin que plusieurs compétences soient impliquées. (ICCI, 2017)

3.9. Choisir la fréquence et le temps de déroulement de l'audit

Les intervalles de réalisation des audits ne doivent pas dépasser les deux ans, a priori. A l'instar de ce temps d'intervalle, le temps de l'audit opéré ne doit pas aller au-delà d'un mois. (ICCI, 2017)

« Quelques étapes clés peuvent par ailleurs être identifiées :

- Fixer les objectifs ;
- Comprendre et cartographier le système ;
- En identifier les forces et les faiblesses ;
- Émettre les recommandations pour en réduire les faiblesses et optimiser les forces. » (ICCI, 2017, slide 45)

3.10. Ne pas sous-estimer les limites d'un audit

Un audit n'est pas à 100 % fiable et sans erreurs, il est évident qu'il subsiste toujours un doute dans l'identification de toutes les faiblesses et éventuelles menaces d'un processus que ce soit lors de la réalisation d'un audit financier en milieu informatique ou non. Il y a des contraintes et des limites qui sont probables comme : un temps limité dans la réalisation de l'audit, ou encore une évaluation floue du contexte fonctionnel de l'organisation auditée. (ICCI, 2017)

Retenons tout de même qu'un auditeur financier n'est pas un informaticien. Quand les procédés s'avèrent être compliqués ou incompréhensibles pour lui, il peut faire appel à des experts afin de l'aider dans son travail.

4. Les normes ISA régissant le travail de l'auditeur et ses particularités

Les normes qui régissent le travail de l'auditeur sont diverses, variées et nombreuses qui plus est. Les deux normes (ISA) que nous traiterons sont les suivantes : l'ISA 315 et l'ISA 265. Les deux normes s'appliquent à tous types d'audit, que ce soit en milieu informatique ou non.

4.1. Norme ISA 315 (révisée), Compréhension de l'entité et de son environnement aux fins de l'identification et de l'évaluation des risques d'anomalies significatives

4.1.1. Objectifs et évaluation des risques

Cette norme ISA nous montre que l'auditeur a pour objectif d'obtenir une compréhension de l'entité et de l'environnement de celle-ci dans son ensemble. Il doit également avoir une compréhension du contrôle interne de l'entité. En ayant une idée claire de ces différents points, l'auditeur pourra déterminer et évaluer les possibles risques d'anomalies significatives. (Nifccanada, 2012)

Les risques pouvant résulter d'erreurs ou de fraudes, que ce soit au niveau des états financiers ou des assertions, le but étant de disposer d'une base pour mettre en place des réponses à l'évaluation qu'il aura faite des risques d'anomalies significatives. (Nifccanada, 2012)

Afin d'évaluer les risques, l'auditeur doit intégrer dans ses procédures d'évaluation les éléments suivants :

Il doit :

- demander des informations auprès de la direction, ou encore avec les personnes adéquates au sein de l'activité d'audit interne (si du moins la fonction existe) mais aussi avec d'autres personnes de l'entité qui peuvent être en possession d'informations pouvant aider l'auditeur à découvrir les différents risques d'anomalies significatives ;
- procéder à la mise en place de procédures analytiques ;
- réaliser des tests physiques et des inspections. (Nifccanada, 2012)

4.1.2. Processus d'évaluation des risques par l'entité

Avant de définir lui-même les risques, l'auditeur doit d'abord déterminer si l'entité qu'il contrôle possède un processus pour :

- Pouvoir, en fonction des objectifs, identifier les risques d'entreprise auxquels ils devront donner de l'importance ;
- Avoir une idée de l'ampleur des risques ;
- Déterminer la probabilité que les risques viennent à se réaliser ou non ;
- Prendre en compte des mesures qui serviront de réponse aux risques. (Nifccanada, 2012)

À partir du moment où l'entreprise a mis en place un « processus d'évaluation des risques par l'entité », l'auditeur devra obtenir une compréhension de celui-ci et des résultats connexes. Il se peut que l'auditeur soit amené à identifier des risques d'anomalies significatives que l'entité n'a pas identifiés via les processus mis en place. Si c'est le cas, l'auditeur devra se poser des questions quant à l'existence d'un risque sous-jacent qui aurait dû être identifié au préalable par la direction. Toujours dans cette optique où la direction a échoué dans la détection d'un éventuel risque, l'auditeur doit trouver une explication au fait que ce risque n'ait pas pu être identifié, de là il évaluera également si le processus est adapté ou bien s'il existe une défaillance assez importante du contrôle interne vis-à-vis du processus d'évaluation des risques. (Nifccanada, 2012)

Il se peut que le management n'ait pas les compétences pour détecter un éventuel risque ou bien qu'il soit passé outre celui-ci. Supposons qu'une entreprise adopte un nouveau logiciel et

que dans l'identification des risques il n'ait pas pris en considération qui avait accès à l'outil. La direction ? Les employés ? Toute l'organisation ? Cela représente un risque dans la mesure où tout un chacun peut entrer dans le logiciel et modifier le contenu des imputations encodées.

Lorsque l'entreprise n'a pas procédé à l'établissement d'un tel processus, l'auditeur devra prévoir des entretiens avec la direction afin de déterminer si les risques d'entreprise auxquels une importance particulière doit être portée en fonction des objectifs ont pu être identifiés et quelles sont les différentes mesures qui ont été prises afin de répondre à ces risques. Il devra également considérer l'absence de processus d'évaluation des risques. Il doit évaluer si cette absence est appropriée dans les circonstances confrontant l'entité ou bien si elle représente une faille importante du contrôle interne. (Nifccanada, 2012)

En ce qui concerne les systèmes d'information, l'auditeur doit également les comprendre, en connaître les usages et fonctionnalités mais aussi acquérir une compréhension des processus opérationnels connexes. L'auditeur doit donc comprendre :

- Les différents types d'opérations qui sont conclues dans le cadre des activités de l'entreprise et qui relèvent d'un caractère important lié aux états financiers ;
- Toutes les procédures que l'entreprise suit, que ce soit dans des systèmes manuels ou des systèmes informatiques, afin de déclencher, d'enregistrer, de traiter, de corriger si nécessaire, de reporter au grand livre général et de communiquer les opérations dans les états financiers ;
- Les pièces justificatives, soit les documents comptables ou tout type d'information justificative et les comptes spécifiques compris dans les états financiers. Il s'agit donc de toute pièce justificative liée aux opérations de l'entité. Les documents peuvent être conservés soit sous format papier, soit électroniquement ;
- La manière dont le système informatique traite les événements, outre les opérations habituelles, importants pour les états financiers ;
- Quel est le processus qui est utilisé afin de préparer les états financiers de l'entreprise, en ce compris les appréciations comptables ou les informations qui sont importantes à fournir ;
- Les différents contrôles annexes aux écritures comptables, mais aussi les écritures « non courantes » qui servent à observer les opérations ou ajustements non récurrents ou inhabituels. (Nifccanada, 2012)

4.2. Norme ISA 265, Communication des déficiences du contrôle interne aux responsables de la gouvernance et à la direction

4.2.1. Objectifs

L'auditeur a pour but de communiquer de la façon la plus adéquate avec les responsables de la gouvernance mais également à la direction. L'auditeur communiquera donc les défaillances qu'il aura pu relever pendant son travail d'audit, et qui donnent raison de les estimer suffisamment inquiétantes et d'y accorder une attention particulière. (Nifccanada, 2009)

« Dans les normes ISA, on entend par :

- « Déficience du contrôle interne », l'une ou l'autre des situations suivantes :
  - Un contrôle est conçu, mis en place ou fonctionne d'une manière telle qu'il ne permet pas de prévenir, ou de détecter et corriger, les anomalies dans les états financiers en temps opportun,
  - Un contrôle nécessaire pour prévenir, ou détecter et corriger, les anomalies dans les états financiers en temps opportun est absent ;
- « Déficience importante du contrôle interne », une déficience ou une combinaison de déficiences du contrôle interne qui est suffisamment préoccupante, selon le jugement professionnel de l'auditeur, pour nécessiter l'attention des responsables de la gouvernance. » (Nifccanada, 2009, p. 4)

4.2.2. Exigences

Il faut que l'auditeur puisse déterminer à la fin de son travail d'audit si ce dernier lui a donné la possibilité de relever une ou plusieurs défaillances du contrôle interne de l'entité auditée. (Nifccanada, 2009)

Lorsque c'est le cas et que l'auditeur a donc pu relever une ou plusieurs faiblesses dans le contrôle interne, il devra déterminer – et ce sur base des différents tests qu'il aura effectués au préalable – si ces faiblesses peuvent constituer, à titre individuel ou collectif, des défaillances lourdes de conséquences. (Nifccanada, 2009)

Supposons que l'entreprise n'ait pas pour l'habitude d'effectuer un backup quotidien des informations qu'elle traite sur un autre serveur que celui utilisé habituellement, cela pourrait s'avérer désastreux en cas de crash informatique.

Des règles existent comme le fait que l'auditeur doit communiquer (avec les personnes concernées, voir point 3.2.1.), et ce en temps utile, les défaillances sérieuses du contrôle interne que celui-ci aura pu relever tout au long de ses travaux d'audit (Nifccanada, 2009). Ceci se fait dans le but de les tenir au courant de l'avancement des travaux et de faire rapport des éléments trouvés.

« L'auditeur doit aussi communiquer en temps opportun à la direction, au niveau hiérarchique approprié :

- Par écrit, les déficiences importantes du contrôle interne qu'il a communiquées ou qu'il entend communiquer aux responsables de la gouvernance, à moins qu'il ne soit pas approprié, dans les circonstances, de communiquer directement avec la direction ;
- Les autres déficiences du contrôle interne relevées au cours de l'audit qui n'ont pas déjà été communiquées à la direction par d'autres parties et qui, selon le jugement professionnel de l'auditeur, sont suffisamment préoccupantes pour nécessiter l'attention de la direction. » (Nifccanada, 2009, p. 5)

« Dans sa communication écrite faisant état des déficiences importantes du contrôle interne, l'auditeur doit fournir :

a. Une description des déficiences et de leurs incidences potentielles ;
b. Des informations suffisantes pour permettre aux responsables de la gouvernance et à la direction de comprendre le contexte de la communication.

   À cet égard, l'auditeur doit notamment préciser :

   i) Que l'audit avait pour objectif l'expression d'une opinion par l'auditeur sur les états financiers,
   ii) Que l'audit a comporté la prise en considération du contrôle interne portant sur la préparation des états financiers afin de concevoir des procédures d'audit appropriées aux circonstances, et non dans le but d'exprimer une opinion sur l'efficacité du contrôle interne,

iii) Que sa communication se limite aux déficiences qu'il a relevées au cours de l'audit et qui, selon lui, étaient suffisamment préoccupantes pour nécessiter leur communication aux responsables de la gouvernance. » (Nifccanada, 2009, p. 6)

4.3. Autres normes

Les normes présentées ci-avant sont des normes internationales qui régissent le travail d'auditeur et celui-ci les connait bien. Cependant en matière d'audit en milieu informatique, les normes ISACA existent et régissent les différentes activités des auditeurs des systèmes informatiques. Si beaucoup de ces normes ISACA ressemblent de près aux normes ISA, nous pouvons relever quelques particularités qui sont propres à l'audit en milieu informatique.

4.3.1. Norme d'audit et d'assurance des SI 1201 – Planification de la mission

« Les professionnels de l'audit et de l'assurance des SI doivent planifier chaque mission d'audit et d'assurance des SI de manière à prendre en compte :

- Le ou les objectifs, la portée, le calendrier et les réalisations
- Le respect des lois applicables et des normes d'audit professionnel
- L'utilisation d'une approche fondée sur le risque, lorsque cela se justifie
- Les questions propres à la mission. » (ISACA, 2013, p. 2)

« Les exigences en matière de documentation et de présentation de rapports Les professionnels de l'audit et de l'assurance des SI doivent élaborer et documenter un plan de projet de mission d'audit ou d'assurance des SI qui décrive :

- Nature, objectifs, calendrier et besoins en ressources de la mission
- Calendrier et portée des procédures d'audit nécessaires pour achever la mission. » (ISACA, 2013, p. 2)

4.3.2. Norme d'audit et d'assurance des SI 1202 – Évaluation du risque dans la planification

« La fonction d'audit et d'assurance des SI doit utiliser une approche d'évaluation du risque et une méthodologie à l'appui appropriées pour élaborer le plan général d'audit des SI et définir les priorités en vue d'une allocation efficace des ressources d'audit des SI. » (ISACA, 2013, p. 2)

« Les professionnels de l'audit et de l'assurance des SI doivent identifier et évaluer les risques pertinents eu égard au domaine examiné lors de la planification de chaque mission. » (ISACA, 2013, p. 2)

« Les professionnels de l'audit et de l'assurance des SI doivent prendre en considération le risque lié à l'objet, le risque d'audit et l'exposition connexe au risque de l'entreprise. » (ISACA, 2013, p. 2). Le risque lié à l'objet de l'audit correspond au domaine qui est examiné. On peut être confrontés par exemple à un risque commercial comme la solvabilité des clients, ou un risque lié à un éventuel projet comme les ressources ou encore la méthodologie utilisée.

Ce que nous retiendrons de cette norme est que les auditeurs doivent évaluer au préalable le risque qui est lié au domaine qu'ils examinent. Lorsque ceci est fait, l'auditeur tentera de réduire le Risque d'audit et rapprochera au maximum celui-ci d'un niveau « acceptable » (ISACA, 2013)

Le risque d'audit est d'aboutir à une conclusion erronée sur base des travaux effectués. Les composantes de ce risque sont :

- Risque de contrôle : c'est-à-dire le risque qui n'aurait pas été détecté par le système de contrôle interne.

  Par exemple : Le risque contractuel, comme en matière de prix ou de pénalités qui n'ont pas été correctement relevés par le contrôle interne.
- Risque de non-détection

  « Le risque que les procédures de corroboration du professionnel de l'audit ou de l'assurance des SI ne détectent pas une erreur susceptible d'être importante, seule ou combinée à d'autres erreurs. » (ISACA, 2013, p. 3)

- Risque inhérent (donc celui lié à l'objet de l'audit)
  Par exemple : Le risque commercial, c'est-à-dire l'insolvabilité ou encore l'incapacité des clients à payer.

Il est important également de savoir que lorsque l'on réalise une procédure d'audit des Systèmes Informatiques, plus le seuil de matérialité sera petit, plus les attentes de l'audit seront précises et le risque d'audit sera important. Afin de pouvoir diminuer le « risque de matérialité accrue », l'auditeur devra réaliser une compensation : soit il augmentera les tests des contrôles (et ainsi réduira le risque de contrôle), soit il étendra les procédures de test de corroboration (pour qu'il puisse ainsi réduire le risque de non-détection) afin de décrocher des garanties ou assurances supplémentaires. (ISACA, 2013)

4.3.3. Norme d'audit et d'assurance des SI 1207 – Irrégularités et actes illégaux

« Les professionnels de l'audit et de l'assurance des SI doivent considérer le risque d'irrégularités et d'actes illégaux pendant la mission. » (ISACA, 2013, p. 2)
Par exemple : Le management override qui consiste en l'abus de pouvoirs de la part de la direction, ou encore un cas de fraude au sein de l'entreprise.

« Les professionnels de l'audit et de l'assurance des SI doivent conserver une attitude de scepticisme professionnel pendant la mission. » (ISACA, 2013, p. 2)

« Les professionnels de l'audit et de l'assurance des SI doivent documenter et communiquer toute irrégularité matérielle ou acte illégal à la partie concernée dans les meilleurs délais. » (ISACA, 2013, p. 2)

Il est essentiel que les auditeurs soient conscients du fait que les différentes erreurs matérielles qu'ils trouvent lors de l'exécution de l'audit des comptes peuvent être liées à des irrégularités ou des actes illicites. Il faut dès lors que l'auditeur acquière une bonne compréhension de la société et de l'environnement dans lequel elle se développe. (ISACA, 2013)

Il rassemblera également tout au long de son audit des éléments probants dans l'optique de déterminer si l'administration ou n'importe quel autre membre du personnel de l'entreprise a des informations sur les irrégularités ou les éventuels actes illégaux. (ISACA, 2013)
L'auditeur cherchera à obtenir de la part de l'entité auditée les différents journaux comptables, les confirmations de soldes clients-fournisseurs par exemple. Ces éléments constituent des documents probants et sont obtenus à la demande du client ou de l'auditeur.

L'idée est que l'auditeur devra également procéder à une étude des comportements, relations et agissements inhabituels. Il faudra également procéder à l'exécution de procédures qui ont pour but de tester le caractère approprié des contrôles internes. Ainsi l'auditeur pourra également déterminer le risque de contournement par tout membre de la société (direction ou autre). (ISACA, 2013)

L'auditeur doit obtenir les éléments suivants :

- « La reconnaissance de la responsabilité de la direction dans l'élaboration et la mise en œuvre de contrôles internes visant à prévenir et à repérer les irrégularités ou les actes illégaux ;
- La divulgation des résultats pertinents de toute évaluation des risques indiquant que des erreurs, des déficiences du contrôle ou des anomalies peuvent exister par suite d'une irrégularité ou d'un acte illégal ;
- La divulgation de la connaissance par la direction d'irrégularités et d'actes illégaux affectant l'entreprise en relation avec la direction et les employés ayant des rôles importants dans le contrôle interne ;
- La divulgation de la connaissance par la direction de tout soupçon d'irrégularité et d'acte illégal affectant l'entreprise, tels que communiqués par des employés, anciens employés, organismes de réglementation et autres. » (ISACA, 2013, p. 2)

Partie 3 : Le cas Excellium Solution SPRL

Le but de cette partie est de réaliser une analyse de risque au sein de l'entreprise Excellium Solution. Il s'agit d'une fiduciaire qui s'occupe de plusieurs dossiers comptables et qui a passé le cap de la digitalisation des processus. Pour la réalisation de cette partie, nous avons organisé un entretien avec le gérant du cabinet. Lors de cette entrevue, nous avons identifié les processus clefs de l'entreprise avec l'aide de Mr. van Aerssen et avons déterminé les risques auxquels l'entreprise est exposée.

Nous prendrons, pour réaliser cette analyse de risques, le modèle présenté précédemment et qui a été établi par l'Institut des Réviseurs d'Entreprises. L'objectif final de cette partie est d'arriver à déterminer les processus financiers qui posent problème et nous tâcherons d'améliorer l'exécution de ceux-ci.

1. Première étape : Identification de l'entreprise et des processus

Nous sommes donc partie à la rencontre de Mr. Xavier van Aerssen, qui est gérant de la société Excellium Solution SPRL. Grâce au modèle de question définies par l'Institut des Réviseurs d'Entreprises, nous avons procédé à la réalisation d'une analyse de risques et avons discuté des éventuelles possibilités afin de corriger les processus qui pourraient poser problème à l'organisation.

Le cabinet comptable est situé à Uccle en région bruxelloise et est composé actuellement d'un gérant, un associé et de quatre employés comptables.

1.1. La performance

Le premier P, consistait en l'analyse de la performance de l'entreprise au travers de questions sur la mission, la stratégie, les valeurs et les objectifs.

Excellium Solution s'occupe de l'accompagnement comptable et fiscal de son portefeuille clients. La mission globale de l'entreprise est de fournir un service de qualité, tant sur le point de vue comptable que sur le point de vue fiscal. La fiduciaire s'occupe également de la

création d'entreprise, toute personne désireuse de créer sa société peut faire appel à ses services.
L'entreprise a pour objectif de voir son effectif s'agrandir. Après discussions, nous sommes arrivés à la conclusion qu'il n'y avait pas réellement de plan sur le long-terme. En fonction de chaque année courue, l'entreprise revoit ses objectifs. Pour 2017, l'objectif principal était l'engagement d'un nouveau membre du personnel.

En termes de valeurs, le cabinet comptable prône des valeurs familiales. Il s'agit en fait d'une petite structure qui se veut chaleureuse et accueillante. Bien évidemment, outre le fait d'être une équipe assez jeune et dont les valeurs sont pro-familiales, nous retrouvons des caractéristiques communes à de nombreuses entreprises telles que : la rigueur, le scepticisme, le perfectionnisme, etc.

Afin de mesurer les performances de l'organisation, les membres du personnel et la direction utilisent un programme appelé Syneton qui leur permet d'enregistrer les prestations pour chaque client. Syneton ressemble de près à un dossier permanent virtuel où l'on retrouve toutes les données clients et chaque service rendu au client. Chaque membre de l'organisation dispose d'un login et d'un mot de passe lui permettant d'encoder ses prestations. L'enregistrement des prestations permet de calculer la rentabilité des dossiers, le cabinet comptable a la possibilité de déterminer les clients rentables ou les clients moins rentables. Ceci leur permet de prendre des décisions plus ou moins graves concernant un éventuel frein aux relations avec un ou des clients.

La rentabilité n'est pas calculée chaque mois, l'état concernant chaque client est réalisé en fin d'année – généralement en même temps que la clôture de l'exercice comptable – et permet ainsi d'avoir un œil critique sur un ensemble d'exercice comptable et pas sur une prestation particulière.

1.2. Postes

Nous avons procédé à l'analyse du bilan déposé à la Banque Nationale de Belgique afin de relever les postes importants de l'entreprise sur l'exercice comptable 2015. Les données sont directement extraites du bilan déposé et ont été commentées avec Mr. Van Aerssen.

ACTIF	Ann.	Codes	Exercice	Exercice précédent
ACTIFS IMMOBILISÉS		20/28	**99.294**	**141.159**
Frais d'établissement		20		
Immobilisations incorporelles	5.1.1	21	**93.161**	**133.639**
Immobilisations corporelles	5.1.2	22/27	**6.133**	**7.520**
Terrains et constructions		22		
Installations, machines et outillage		23		
Mobilier et matériel roulant		24	6.133	7.520
Location-financement et droits similaires		25		
Autres immobilisations corporelles		26		
Immobilisations en cours et acomptes versés		27		
Immobilisations financières	5.1.3/5.2.1	28		

Banque Nationale de Belgique. (2016). Comptes annuels Excellium Solution SPRL. Récupéré le 2 mai 2017 de https://cri.nbb.be/bc9/web/catalog;jsessionid=0B2E0F58B27126E620F9C59EA0415BA0?execution=e1s1

En matière d'actifs immobilisés, l'entreprise dispose d'immobilisations incorporelles qui sont assez importantes. Il s'agit en réalité d'un Goodwill qui correspond à un rachat de clientèle en 2009.

ACTIFS CIRCULANTS		29/58	**117.726**	**150.140**
Créances à plus d'un an		29		
Créances commerciales		290		
Autres créances		291		
Stocks et commandes en cours d'exécution		3		
Stocks		30/36		
Commandes en cours d'exécution		37		
Créances à un an au plus		40/41	**104.262**	**120.910**
Créances commerciales		40	103.868	117.860
Autres créances		41	394	3.050
Placements de trésorerie	5.2.1	50/53		
Valeurs disponibles		54/58	**11.291**	**27.016**
Comptes de régularisation		490/1	**2.173**	**2.214**
TOTAL DE L'ACTIF		20/58	**217.020**	**291.299**

Banque Nationale de Belgique. (2016). Comptes annuels Excellium Solution SPRL. Récupéré le 2 mai 2017 de https://cri.nbb.be/bc9/web/catalog;jsessionid=0B2E0F58B27126E620F9C59EA0415BA0?execution=e1s1

Dans les actifs circulants, le poste qui ressort le plus est celui des créances commerciales. Celui-ci est de cette importance dû au système de facturation de l'entreprise. Les factures sont établies et envoyées aux clients entre le 15 et le 20 du mois de décembre. Ceci fait que lorsque les comptes sont arrêtés au 31 décembre de chaque année, les factures du mois de décembre pour les mensuels et les factures du quatrième trimestre pour les trimestriels ne sont pas toutes réglées.

Pour ce qui est du délai de paiement client, l'entreprise accorde 15 jours vu qu'il s'agit d'une facturation à l'heure et d'un service qui est déjà presté avant établissement de la facture.

DETTES		17/49	**141.886**	**220.344**
Dettes à plus d'un an	5.5	17	**3.151**	**36.322**
Dettes financières		170/4	3.151	36.322
Etablissements de crédit, dettes de location-financement et assimilées		172/3	3.151	36.322
Autres emprunts		174/0		
Dettes commerciales		175		
Acomptes reçus sur commandes		176		
Autres dettes		178/9		
Dettes à un an au plus	5.5	42/48	**138.735**	**184.022**
Dettes à plus d'un an échéant dans l'année		42	35.722	53.591
Dettes financières		43		
Etablissements de crédit		430/8		
Autres emprunts		439		
Dettes commerciales		44	48.571	83.060
Fournisseurs		440/4	48.571	83.060
Effets à payer		441		
Acomptes reçus sur commandes		46		
Dettes fiscales, salariales et sociales		45	54.111	47.371
Impôts		450/3	31.127	29.147
Rémunérations et charges sociales		454/9	22.984	18.224
Autres dettes		47/48	331	

Banque Nationale de Belgique. (2016). Comptes annuels Excellium Solution SPRL. Récupéré le 2 mai 2017 de https://cri.nbb.be/bc9/web/catalog;jsessionid=0B2E0F58B27126E620F9C59EA0415BA0?execution=e1s1

Au niveau des passifs, les postes les plus importants se retrouvent parmi les dettes. Nous constatons que les dettes commerciales et les dettes fiscales, salariales et sociales constituent la majeure partie des dettes. L'entreprise se veut compétitive concernant les salaires employés et leur offre de nombreux avantages. Malgré que ce soit une petite structure, les coûts les plus importants sont ceux du personnel.

La fiduciaire est en bonne santé et arrive à dégager du bénéfice. Un bénéfice en 2015 de 27.174 euros contre 23.269 euros en 2014.

Produits et charges d'exploitation					
Marge brute d'exploitation	(+)/(-)		9900	308.795	296.943
Chiffre d'affaires			70		
Approvisionnements, marchandises, services et biens divers			60/61		
Rémunérations, charges sociales et pensions	(+)/(-)	5.6	62	236.201	158.078
Amortissements et réductions de valeur sur frais d'établissement, sur immobilisations incorporelles et corporelles			630	50.711	50.925
Réductions de valeur sur stocks, sur commandes en cours d'exécution et sur créances commerciales: dotations (reprises)	(+)/(-)		631/4		
Provisions pour risques et charges: dotations (utilisations et reprises)	(+)/(-)		635/7		
Autres charges d'exploitation			640/8	1.003	987
Charges d'exploitation portées à l'actif au titre de frais de restructuration	(-)		649		

Banque Nationale de Belgique. (2016). Comptes annuels Excellium Solution SPRL. Récupéré le 2 mai 2017 de https://cri.nbb.be/bc9/web/catalog;jsessionid=0B2E0F58B27126E620F9C59EA0415BA0?execution=e1s1

Au niveau des résultats, nous remarquons que l'entreprise dégage une marge brute d'exploitation d'un montant de 308.795 euros. Comme nous le relevions précédemment, l'entreprise supporte des charges sociales et des rémunérations assez importantes qui représentent pas moins de 76,5 % de sa marge brute d'exploitation. Nous pouvons dès lors conclure que presque tout le bénéfice retiré de l'activité sert à payer les employés.

Les comptes 61 – que nous ne voyons pas sur l'image ci-dessus – sont composés en majeure partie de frais liés à l'informatique avec notamment :

- Cloudbizz ;
- Codabox ;
- Winbooks.

Cloudbizz étant le fournisseur cloud de l'entreprise, Codabox qui récupère les relevés bancaires des clients du cabinet comptable et les met à disposition sous une forme dématérialisée et qui permet l'encodage desdits relevés. Les mises-à-jour Winbooks constituent également une bonne partie des comptes 61.

1.3. Processus

Les comptes annuels de l'entreprise sont établis par le gérant de la société de concert avec son associée. Ils procèdent tous deux à l'établissement des comptes annuels et complètent les annexes aux comptes annuels. Pour ce faire, ils utilisent un logiciel d'analyse bilantaire.

Une fois que les comptes annuels sont approuvés par le gérant et son associée, la secrétaire réalise le dépôt en ligne des comptes annuels sur la BNB et envoie la déclaration à l'impôt des sociétés sous format XBRL (eXtensible Business Reporting Language) sur Biztax qui est un service du Service Public Fédéral FINANCES permettant le dépôt en ligne de la déclaration.

« XBRL est un langage informatique spécialement développé pour l'échange de rapports financiers via Internet. » (Banque Nationale de Belgique, 2017)

Les intervenants sont donc trois personnes ; les deux associés et la secrétaire.

1.4. Programmes

Au niveau des programmes, nous avons relevé quasi la totalité d'entre eux. Etant un bureau comptable, l'entreprise fait appel à un programme de comptabilité qui dans ce cas-ci est Winbooks. Avec ce dernier ils utilisent également Virtual Invoice qui est un programme de reconnaissance de facture et qui leur permet d'attribuer un document à une écriture comptable. Le cabinet utilise également Codabox que nous expliquions précédemment.

1.5. Plateformes

L'entreprise travaille en cloud, ce qui lui permet de se connecter à son bureau virtuel à tout moment et depuis n'importe quel endroit. Il suffit d'avoir une connexion internet et un appareil électronique capable de s'y connecter.

Selon Mr van Aerssen, le cloud leur permet d'avoir un accès facile à la comptabilité des clients de la fiduciaire à n'importe quel moment. Lorsque les comptables se trouvent chez le client le cloud leur permet d'avoir une vue directe sur la comptabilité sans devoir transporter tous les classeurs. Dans le cas où un classeur a été oublié par le comptable, il pourra retrouver toutes les informations nécessaires sur le cloud.
L'entreprise utilise d'autres plateformes comme un site internet où les clients peuvent également y télécharger leurs documents nécessaires à l'encodage de la comptabilité. De plus, le cabinet comptable est également sur les réseaux sociaux avec une page sur Facebook permettant ainsi d'avoir un champ d'action plus large et atteindre plus de personnes car nous savons que de nos jours presque tout le monde est inscrit sur les réseaux sociaux et il s'agit là d'un moyen de communication avec le grand public.

1.6. Processus de gérance IT

En 2012, l'entreprise a subi un crash sur son serveur local qui a entraîné la perte d'une grande partie des données qui étaient sur le serveur. Il y a eu 30% des dossiers qui avaient perdu au moins six mois d'encodage. La récupération des données fut un processus assez long qui a demandé beaucoup de travail aux membres du personnel. Suite à ce problème, la gérance a décidé de passer au travail sur cloud.

En matière de continuité, l'entreprise ne dispose pas de back-up externe autre que celui qui est enregistré sur le cloud. Un tel back-up prendrait environs 36 heures à l'entreprise. Le principe de continuité est celui selon lequel l'entreprise peut continuer ses activités si les différents programmes ne fonctionnent plus. En réalité il s'agit de la « roue de secours » de l'entreprise, si celle-ci n'avait plus l'outil habituel qu'elle utilise comment ferait-elle ? Aucun processus n'a été prévu afin de contrer un quelconque problème impactant la continuité des activités. N'ayant pas encore subi ce genre d'arrêt complet qui nécessiterait un moyen autre que le cloud pour continuer ses activités, l'entreprise n'a pas ressenti le besoin de prévoir une solution éventuelle.

Toutefois, l'entreprise est souvent confrontée à des petits dérangements liés au cloud computing. Il arrive que le cloud bloque l'espace de quelques minutes obligeant les utilisateurs à se déconnecter puis à se reconnecter. Effectivement, la procédure de déconnexion et de reconnexion au cloud est répétitive et ennuyante pour les employés lorsqu'ils sont confrontés à plusieurs bugs sur la journée, cependant la rentabilité n'en est pas affectée selon le gérant. Selon lui, les différentes pertes de temps que connaissent les employés au bureau sont récupérées par une possibilité de connexion chez le client et d'une connexion à distance (depuis le domicile par exemple).

Au niveau du management et des changements affectant celui-ci, les procédures sont assez bien définies. Il y a un peu plus d'un an la gestion de l'entreprise était entre les mains de deux gérants associés et d'une troisième associée. Suite à une restructuration et la séparation des gérants, le cabinet comptable a procédé à la suppression des différents accès dont disposait le second gérant. Mr. van Aerssen a procédé à la suppression de :

- L'adresse mail ;
- L'accès CloudBizz ;
- L'accès Winbooks ;
- La gestion des mandats bancaires ;
- Le référencement ONSS (Office National de Sécurité Sociale) qui gère les accès à Tax On Web et MyMinfin.

La fiduciaire a également fait toutes les démarches afin de rayer le nom de l'ancien gérant-associé afin que tout soit conforme. Le cabinet dispose également d'une carte Isabel (système

de paiement multibancaire pour les professionnels), l'ancienne fut supprimée et une nouvelle fut commandée.

Un point important à relever, toujours selon les questions de l'Institut des Réviseurs d'Entreprises, est la sécurité. Tous les accès aux outils informatiques sont protégés par un login et un mot de passe. Afin de se connecter au cloud, chaque membre du personnel a un login et un mot de passe pour s'y connecter. Pour procéder à l'encodage sur le programme comptable, chaque membre détient également un nom d'utilisateur et un mot de passe. Certains accès requièrent l'accès avec la carte d'identité notamment pour les plateformes en ligne de l'administration.

2. Deuxième étape : Analyse des risques identifiés

Après avoir identifié les processus clefs de l'entreprise, nous avons pu discuter des différents risques que cette dernière encourt. Les risques sont répertoriés, encore une fois, en fonction du modèle de l'Institut des Réviseurs d'Entreprises.

2.1. Risque Business

Au niveau des risques business, nous avons relevé un risque de responsabilité professionnelle. Il se peut, qu'à un moment ou un autre, le cabinet soit amené à donner un faux ou mauvais conseil. En tant que chef d'entreprise, Mr. van Aerssen a souscrit à une assurance responsabilité professionnelle. Cette assurance permet d'être couvert en cas de dommage causé à un tiers par l'exercice des activités de l'entreprise. Le cabinet comptable n'est pas à l'abri d'un retournement d'un client pour un éventuel mauvais traitement de sa comptabilité.

Certaines erreurs ne sont pas couvertes par les assurances, par exemple lors d'une erreur de délai de rentrée des documents. Il s'agit d'un risque non couvert par une assurance et qui engage la responsabilité professionnelle d'Excellium Solution.

2.2. Risque comptes annuels

Il est difficile d'identifier un risque éventuel au niveau des comptes annuels car il s'agit d'un bureau comptable et qu'ils y sont habitués, cependant le risque zéro n'existe pas ! La Banque

Nationale de Belgique procède à des contrôles arithmétiques et logiques, ce qui évite les éventuelles erreurs comme une mauvaise addition des actifs immobilisés par exemple. La fiduciaire n'est pas à l'abri d'une mauvaise manipulation lors de la préparation des comptes annuels. Toutefois, l'entreprise a la possibilité de rectifier les comptes annuels lors de la détection d'une erreur éventuelle.

Cependant, l'entreprise ne peut pas tout corriger !
« La règle est que les sociétés sont autorisées à rectifier des erreurs matérielles commises dans l'établissement des comptes annuels, mais elles ne peuvent pas corriger ce qui est à considérer comme une erreur résultant d'une 'décision de gestion'.
Selon l'administration fiscale, il ne faut évidemment pas que la société en vienne à adapter son bilan, et dans la foulée dépose une déclaration fiscale rectificative, parce qu'elle se rend compte que le bilan déposé ne prend pas en compte un avantage fiscal auquel elle n'avait à l'époque pas songé. » (Coppens, 2014, p. 31)

Nous considérerons dès lors qu'il existe un risque, certes moins récurrent mais toutefois probable, que l'entreprise fasse un dépôt erroné et que la rectification désirée ne soit pas admise car « non matérielle ».

2.3. Risque processus

En ce qui concerne les risques processus, nous avons pu identifier deux risques.

L'entreprise donne l'opportunité aux membres du personnel d'être assez autonomes dans la gestion de la comptabilité des dossiers. Un membre du personnel peut se charger de la comptabilité A à Z d'un dossier sans que le superviseur ne vérifie le travail effectué. Il n'y a pas de processus mis en place afin que le superviseur puisse repasser sur le dossier afin de vérifier toute la comptabilité. Il faut savoir que l'entreprise travaille en plateau, employés et gérant confondus, ce qui permet aux comptables de poser leurs questions directement à leur supérieur. Par conséquent, d'une certaine façon, les dossiers sont également suivis par le superviseur.

Nous avons également relevé un risque provenant de la communication. Il arrive que lors de l'acceptation d'un nouveau client, le gérant n'ait pas encore prévu quel employé serait le

gestionnaire du dossier. Le gérant assiste donc seul à la réunion de présentation, si nous pouvons l'appeler ainsi. Il n'y a pas de procédure mise en place afin de réaliser un compte-rendu de la réunion pour que le gestionnaire de dossier ait les informations nécessaires à l'établissement d'une comptabilité adéquate. Il existe donc un risque de mauvaise communication interne. Il s'agit d'un risque en interne qui peut se répercuter sur un risque probable avec les parties externes dont le client.

2.4. Risque programmes

Concernant les programmes le risque majeur que nous pouvons relever est que l'entreprise perde des données dû à une erreur humaine. La perte de données constitue un des risques les plus importants d'une fiduciaire. Perdre un mois d'encodage n'est pas très grave en soi, supposons que l'entreprise soit à nouveau confrontée à une perte de donnée équivalente à celle qu'elle a connu en 2012 avec plusieurs mois de perdu.

2.5. Risque plateformes

Pour commencer, prenons le cloud. L'entreprise entrepose une quantité considérable d'informations sur ses clients. Il serait fort dommageable pour l'entreprise si un hacker venait à craquer la sécurité du cloud et qu'il fasse usage des informations trouvées. Le risque de hacking est donc bien présent malgré qu'on n'en entende pas beaucoup parler.

L'avantage du cloud est que celui-ci dispose de plusieurs serveurs qui ne sont pas localisés au même endroit, et ses serveurs enregistrent des copies des données constamment. On appelle cela des serveurs miroir, c'est-à-dire des serveurs qui sont la copie identique les uns des autres. La probabilité est extrêmement faible qu'un hacker prenne en « otage » les données de l'entreprise sur tous les serveurs en même temps. Ce qui fait que l'entreprise pourra toujours réclamer l'ensemble de ses données.

Nous relèverons également que le fait qu'Excellium Solution ne soit pas le seul maître de ses données comporte un risque assez important. L'entreprise passe par un informaticien indépendant qui s'avère travailler avec Cloudbizz, ce qui fait que trois parties prenantes ont accès aux informations sur le cloud :

1. L'informaticien

2. Cloudbizz
3. Les membres du personnel

L'information bien que confidentielle est tout de même partagée entre différents acteurs. Les informations sont hébergées sur les serveurs de Cloudbizz, gérées par informaticien et utilisées par le cabinet comptable. L'informaticien devient le maître suprême des accès de l'entreprise ! De plus, l'entreprise a très peu de garanties sur l'utilisation qu'est faite de toutes les données qui sont entreposées sur le cloud.

Un autre problème qui peut se poser est lié à la localisation des serveurs du cloud. Comme nous le remarquions précédemment, les serveurs se trouvent dans différents pays. Des problèmes juridiques peuvent se poser puisque les entreprises ne savent pas toujours où les informations sont localisées précisément. Outre le manque de précision concernant la localisation, nous ne savons pas toujours à quelles lois sont soumises nos informations. Prenons l'exemple des Etats-Unis, le président est soumis à la loi du Patriot Act de son nom complet : « Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ». Cette loi permet au président des Etats-Unis d'Amérique d'avoir accès à toutes les informations sur son territoire s'il en juge nécessaire. Il y a peu de chances que les données d'Excellium Solution intéressent le président des Etats-Unis mais cet exemple est représentatif de la législation des pays étrangers qui peut être différente de la nôtre.

Le cloud permet une connexion depuis un endroit quelconque du moment que l'on dispose d'un accès internet. Supposons qu'un employé se connecte à un ordinateur public pour lire ses mails et qu'il oublie de fermer sa session après utilisation. La connexion à distance comporte également ses inconvénients bien qu'il soit plus rare (voire même que cela n'arrive jamais) qu'un employé se connecte sur un ordinateur public. Cela peut avoir des conséquences graves pour l'entreprise.

2.6. Risque processus IT

Lors de l'analyse de la sécurité informatique du cabinet, nous avons relevé le fait que ces derniers avaient les mêmes mots de passe pour quasi toutes les applications. De plus, tous les employés ont le même mot de passe. Cela comporte un risque dans le sens où un hacker

aillant trouvé le mot de passe d'une session cloud pourra trouver celui des autres. Le problème n'est pas seulement lié à un hacker qui prendrait possession d'une session ou l'autre, le problème peut venir du personnel en interne. Chaque employé a accès aux sessions des autres travailleurs car tous les logins sont similaires et les mots de passe identiques. Il se pourrait qu'un employé ait de mauvaises intentions et accède à la session de son collègue afin de l'utiliser pour de mauvaises raisons.

Concernant la facturation, le gérant ne vérifie pas les factures établies par la secrétaire. Il est déjà arrivé qu'une facture ait été mal établie, mais ce type d'événements est sporadique. Ce n'est arrivé qu'une seule fois en l'espace de trois années. Malgré tout nous devons attirer l'attention d'Excellium Solution sur le fait que le fait que la secrétaire envoie les factures sans approbation de la direction comporte un risque.

Le plus gros risque que nous constatons dans les processus IT concerne le back-up externe. Le back-up externe représente une sécurité pour l'entreprise afin d'assurer une continuité d'activités. Si le cloud est attaqué ou si le cloud subi une panne générale, le cabinet ne peut pas continuer ses activités. L'entreprise n'a pas prévu de plan de secours et cela représente un risque majeur pour la fiduciaire. Dans le cas de perte de données, un back-up externe permettrait à l'entreprise de continuer ses activités en récupérant les données depuis un serveur externe au cloud.

3. Conseils pour une meilleure gestion des processus

Afin d'améliorer les processus internes à l'entreprise, nous avons réfléchi à différentes façons de gérer le digital au sein de l'organisation.

3.1. La supervision

Le cabinet devrait mettre en place un procédé de vérification du travail effectué par le personnel. En ce qui concerne l'encodage de A à Z des dossiers clients, le fait de travailler en plateau est un bon moyen d'éviter certains problèmes liés à une mauvaise comptabilisation. Les gestionnaires de dossiers sont en contact permanent avec les superviseurs et peuvent dès lors poser leurs questions directement à ceux-ci. Cependant concernant la facturation faite par la secrétaire, il faudrait que le cabinet pense à un système d'approbation des factures. Lorsque

la secrétaire établi la facture, elle la fait parvenir au gérant qui y appose sa signature. Cela permet au gérant d'avoir un suivi sur la facturation et d'approuver tous les frais qui sont facturés au client.

3.2. La communication

La communication est un élément essentiel dans la gestion d'une activité, quelle qu'elle soit ! Mr. van Aerssen nous révélait qu'un des points faibles après une réunion était que la communication ne se faisait parfois pas correctement entre lui-même et les employés. Afin de corriger ce problème nous avons pensé à l'établissement d'un document Word type où certaines informations jugées importantes – comme par exemple le secteur d'activité du client, ses objectifs ou encore sa stratégie – devraient être mentionnées afin de faciliter l'encodage du dossier.

Avec pas moins de 200 clients, il arrive qu'on s'y perde parmi les activités et surtout comment le client veut que son dossier soit géré. En ayant mis au point un système de « compte-rendu », les employés auront plus facile à s'y retrouver.

Récemment, l'entreprise a acquis un nouveau programme permettant d'échanger directement avec le client. Il s'agit en fait d'une plateforme où le client pourrait déposer électroniquement ses documents et interagir directement avec le gestionnaire de dossier ou avec la direction. La digitalisation comporte des risques en matière de sécurisation, cependant dans ce cas-ci l'entreprise aura plus de facilités à communiquer avec les clients et pourra ainsi garantir une meilleure efficacité en matière de gestion de dossier.

3.3. La perte de données

Contre la perte de données l'entreprise doit utiliser la solution la plus viable qui est de réaliser un back-up externe des données qu'elle traite. Beaucoup d'entreprises qui perdent leurs données font faillite dans les mois qui suivent. Si le cabinet comptable venait à perdre la totalité des données elle pourrait ne pas s'en remettre. Afin de contrer une éventuelle perte de données, une entreprise française a créé une box qui s'appelle Wooxo. Il s'agit d'un système de back-up et de récupération de données.

« Wooxo élimine les risques d'interruption d'activité liés à la perte de données informatiques et accroît la productivité des organisations en permettant à leurs collaborateurs d'exploiter les documents professionnels en tout lieu, à tout instant et de façon sécurisée. » (Wooxo)

Cette box permettrait à de nombreuses entreprises de contrer un problème de perte de données ce qui pourrait signifier pour cette dernière un arrêt inopiné des activités. Il s'agit d'un moyen de prévention, quelques peu coûteux certes, mais plutôt efficace.

3.4. La localisation des données

Afin que l'entreprise ne soit pas embarrassée avec des questions ayant attrait à la localisation des données, celle-ci devrait prendre le temps d'analyser et de discuter avec son fournisseur cloud de la localisation des serveurs contenant les informations propres à l'entreprise. L'entreprise pourra alors être rassurée quant aux éventuels désagréments liés à une législation intrusive.

3.5. La sécurité

Le Centre For Cyber Security de Belgique a publié un guide pour les Petites et Moyennes Entreprises désirant se protéger contre la cybercriminalité. Nous n'entrerons pas dans les détails, nous citerons simplement les conseils donnés car ceux-ci sont plutôt explicites et ressemblent fortement à ce que nous déterminions plus tôt lorsque nous abordions la stratégie digitale (cfr. p. 13).

1. « Impliquez le Top Management ;
2. Elaborez une politique de sécurité et un code de conduite ;
3. Sensibilisez vos travailleurs aux risques cyber ;
4. Gérez vos ressources informatiques importantes ;
5. Mettez à jour tous les programmes ;
6. Installez une protection antivirus ;
7. Sauvegardez toutes les informations ;
8. Gérez l'accès à vos ordinateurs et réseaux ;
9. Sécurisez les postes de travail et les appareils mobiles ;
10. Sécurisez les serveurs et les composants de réseau ;

11. Sécurisez les accès à distance ;
12. Disposez d'un plan de la continuité des activités & d'un plan de gestion des incidents. » (Centre For Cyber Security Belgium, 2017, p. 5)

4. L'analyse d'Eric Gryson, CEO de Ricoh Belgium SA

Dans ce point-ci, nous allons relater les éléments essentiels d'une interview réalisée avec le Chief Executive Officer de Ricoh Belgium SA en leurs bureaux le 27 avril 2017. Cette interview s'est opérée dans le but d'avoir un avis externe et professionnel concernant les risques que nous pouvions identifier. De plus, cela permettra également de mettre en exergue d'autres risques auxquels nous n'avons pas pensé lors de l'analyse de risques auprès de la fiduciaire.

Selon Eric Gryson, les grands risques des entreprises d'aujourd'hui sont au nombre de quatre :

1. Le risque de ne pas être une entreprise digitale
2. Le risque de perte de données
3. Le risque de la portabilité
4. Le risque de e-réputation

4.1. Le risque de ne pas être une entreprise digitale

Comme nous le disions précédemment, une entreprise qui ne s'adapte pas à l'ère digitale est une entreprise qui se confronte à des difficultés face aux autres entreprises plus digitalisées. Cela signifie qu'en n'acceptant pas le numérique par crainte de l'inconnu, ou parce que l'entreprise n'en ressent pas le besoin, rend celle-ci moins compétitive par rapport à ses concurrents. Elle peut s'avérer être moins compétitive pour plusieurs raisons, comme par exemple :

- Parce que les processus internes sont obsolètes et entraînent une diminution de l'efficacité ;
- Parce que l'entreprise n'est pas présente sur les réseaux sociaux ou ne dispose pas d'un site internet permettant l'achat de produits.

Le fait de ne pas se digitaliser engendre une perte de clientèle probable, engendre des coûts supplémentaires par le maintien de procédures inefficaces, etc.

4.2. Le risque de perte de données

Nous l'avons également relevé lors de l'analyse de risques faites auprès d'Excellium Solution. Selon E. Gryson, les entreprises sont fort exposées à la perte de données car beaucoup d'entre elles ne disposent pas d'un système de back-up. Il existe un type de back-up que l'on appelle incrémentiel et qui représente une solution de sauvegarde des données par modification, c'est-à-dire que le back-up (qui est parfois une opération très lourde) ne se refait pas à chaque fois ! Le principe du back-up incrémentiel est de sauvegarder les modifications qui ont été faites depuis le premier back-up et venir les ajouter au premier fichier de sauvegarde. Ceci entraîne une diminution du temps de back-up et pourrait être très utile pour Excellium Solution qui nous disait nécessiter 36 heures pour procéder à un back-up.

De plus, le back-up est parfois mal réalisé. Beaucoup d'entreprises procèdent au back-up des données mais peu d'entre elles réalisent un back-up des programmes. Il n'est pas très utile de sauvegarder des données, si les outils permettant de les traiter ne sont pas également sauvegardés.

4.3. Le risque de la portabilité

Le « risque de portabilité » est lié aux possibilités que l'on a en utilisant les différents outils numériques, lié aux « portes ouvertes ». Plus l'entreprise ouvre des portes à des possibles intrusions externes ainsi qu'internes, plus elle encourt des risques.

Par exemple, dans de nombreuses entreprises les dirigeants ne limitent pas les accès à des sites non sécurisés comme les sites de rencontres, sites pornographiques ou autres. Les entreprises s'exposent à des virus, des intrusions externes, à des vols d'identité et d'autres risques provenant de sites suspects.

4.4. Le risque de e-réputation

L'e-réputation et la fidélisation des clients sont deux termes extrêmement liés. Cette réputation en ligne est un élément clef dans le prospect de nouveaux clients puisque ces derniers chercherons des informations concernant l'entreprise sur internet. L'internet est une source importante d'informations pour les clients. Par exemple, les futurs clients aiment consulter les avis des personnes ayant déjà fait appel aux services de l'entreprise. Ces clients peuvent consulter les avis d'anciens clients ou de clients actuels sur le site même de l'entreprise concernée ou par le biais d'autres plateformes, le but étant de se faire une première opinion sur l'entreprise. (Reputation VIP, 2017)

Nous pouvons comparer ce phénomène au bouche-à-oreille traditionnel que l'on connait, sauf qu'il s'agit d'un phénomène dématérialisé et qui est ouvert à un plus grand échantillon de personnes. Avant l'utilisation d'internet pour se renseigner sur une entreprise, nous aurions cherché à connaître la réputation d'une entreprise à travers les échos provenant de l'entourage. Aujourd'hui nous avons accès à une multitude d'avis et commentaires de personnes à travers le monde (comme par exemple les avis et commentaires sur Amazon qui sont rédigés par des milliers de personnes de contrées différentes). Les risques pour l'entreprise sont élevés du fait de cet ensemble d'information, de l'accès rapide à l'information, mais parfois aussi lié au manque de fondement de quelques avis. (Reputation VIP, 2017)

Même si certains des commentaires sont vrais et bien fondés, d'autres commentaires sont basés sur des mensonges dans un but intéressé. Les concurrents peuvent être derrière l'e-réputation de l'entreprise que nous dirigeons et donc faire baisser sa e-réputation. Non seulement cela peut être des commentaires négatifs de la part de nos concurrents mais cela peut être aussi des commentaires positifs de la part des membres du personnel de l'entreprise. Ce procédé n'est donc pas très fiable, les commentaires doivent être lus avec un certain recul car tout n'est pas forcément vrai. (Reputation VIP, 2017)

Ce risque est également lié au risque de portabilité. Continuons avec l'exemple repris ci-dessus des entreprises qui ne bloquent pas les accès à des sites suspects. Peu d'entreprises sont conscientes du fait que Google bloque les interactions de clients probables avec le site internet jugé suspect. E. Gryson a mis en place un blocage de sites indésirables car ce blocage

de la part de Google est un manque à gagner pour son entreprise. Lorsque les sites des entreprises sont bloqués, la communication avec les clients et futurs clients ne se fait pas car les sites sont considérés comme dangereux.

Prenons un exemple pour illustrer cela. Supposons que nous sommes une société (X) de services ayant plusieurs départements et plusieurs membres du personnel. Chaque membre peut se connecter au réseau internet depuis son ordinateur ou de son smartphone. Un employé est actif sur un site de rencontre et consulte ses messages au bureau, donc en utilisant le réseau de l'entreprise. Ce type de site étant considéré comme « dangereux », Google retient que l'entreprise (X) a consulté un site de rencontres (le personnel utilisant le réseau de l'entreprise) et au bout de quelques connexions à de tels sites entraîne une mauvaise réputation de l'entreprise (X).

Conclusion

Les risques de la digitalisation trouvent leurs origines dans différentes sources. Comme nous avons pu le constater, les risques n'émanent pas seulement du fait que l'entreprise procède à une digitalisation de ses procédés. Nous pouvons affirmer que la digitalisation donne de nombreux avantages aux entreprises, et comme le dirait Eric Gryson : « Les risques de la digitalisation sont liés aux avantages qu'elle donne. »

Les PME belges qui adoptent le digital se trouvent confrontées à de nombreux risques qu'il convient d'analyser et d'identifier des possibles solutions pour les contrer. Nous avons pu déterminer les risques liés au personnel, ceux liés au réseau informatique et internet, ceux liés aux législations locales des pays où les serveurs se situent, les risques du cloud, etc. Toutefois, nous reconnaîtrons que le risque le plus important auquel les entreprises font face est la perte de données ! Il faut que les entreprises prévoient des mesures afin d'éviter une telle perte qui pourrait bien causer une cessation fortuite de leurs activités.

Des solutions existent pour se prémunir contre les différents risques, nous en avons fait état de quelques-unes dont Wooxo un système de back-up et de restore des données qui peut être très utile à l'entreprise. Grâce à une analyse minutieuse des risques liés aux différents processus numériques, plateformes numériques, et autres que nous avons développés tout au long du mémoire, l'entreprise pourra faire face à une digitalisation mal abordée.

En quoi une entreprise non-digitale fait, elle, face à moins de risques qu'une entreprise digitale ? Le défi pour les entreprises est d'établir une stratégie digitale de poids qui leur évitera de faire face à des problèmes de taille comme les risques d'intrusion de la part de hackers ou encore les risques sociaux pouvant provenir des employés de la société. Une gestion stratégique, claire et consciencieuse de la numérisation est la clef de la réussite de nos PME belges en milieu digital.

Bibliographie

- Abilways Digital. (2016). *Pourquoi la transformation digitale fait-elle peur aux petites entreprises ?* Récupéré le 15 Avril 2017, sur Abilways Digital: http://www.abilways-digital.com/magazine/pourquoi-la-transformation-digitale-fait-elle-peur-aux-petites-entreprises/

- Alphalives. (2017). *La digitalisation*. Consulté le 29 Avril 2017, sur Alphalives: https://www.alphalives.com/digitalisation/

- Aud-IT. (2012). *Référentiel CobiT*. Consulté le 20 Avril 2017, sur Aud-IT - Audit, sécurité informatique et formation: http://www.aud-it.ch/cobit.html

- Axelor. (2017). *Quelle est la définition d'un ERP ?* Consulté le 28 Avril 2017, sur Axelor: http://www.axelor.com/fr/erp-definition/

- Banque Nationale de Belgique. (2016). Comptes annuels Excellium Solution SPRL. Récupéré le 2 mai 2017, sur Banque Nationale de Belgique: https://cri.nbb.be/bc9/web/catalog;jsessionid=0B2E0F58B27126E620F9C59EA0415BA0?execution=e1s1

- Banque Nationale de Belgique. (2017). *XBRL, c'est quoi?* Consulté le 2 Mai 2017, sur Banque Nationale de Belgique: https://www.nbb.be/fr/centrale-des-bilans/xbrl/xbrl-cest-quoi

- Bastien, L. (2017). *Cloud Computing – Définition, avantages et exemples d'utilisation*. Consulté le 14 Avril 2017, sur Le Big Data: http://www.lebigdata.fr/definition-cloud-computing

- Blanc, X. (2016). *La dette technique expliquée !* Consulté le 29 Mars 2017, sur ProMyze: https://promyze.com/wp-content/uploads/2016/06/LaDetteTechnique.pdf

- Cardoso, J. (2016). *Pourquoi intégrer ou mettre en place un écosystème numérique*. Consulté le 25 Avril 2017, sur Bee My Bees: https://beemybees.com/corporate/mettre-place-ecosysteme-numerique/

- Centre For Cyber Security Belgium. (2017). *Cybersécurité - Guide pour les PME*. Consulté le 27 Avril 2017, sur Centre For Cyber Security Belgium: http://www.ccb.belgium.be/sites/default/files/documents/CCB-FR%20-F.pdf

- Cigref. (2011). *Les risques numériques pour l'entreprise.* Consulté le 19 Février 2017, sur Cigref: http://www.cigref.fr/cigref_publications/RapportsContainer/Parus2011/Risques_numeriques_pour_l_entreprise_CIGREF_2011.pdf

- Commission des Normes Comptables. (2010). *Avis CNC 2010/14 - Conservation des livres et des pièces justificatives.* Consulté le 3 Mai 2017, sur Commission des Normes Comptables: http://www.cnc-cbn.be/files/advice/link/2010-14.pdf

- Commission des Normes Comptables. (2016). *Avis CNC 2016/22 - Conservation des livres et pièces justificatives en cas de tenue de comptabilité informatisée.* Consulté le 3 Mai 2017, sur Commission des Normes Comptables: http://www.cnc-cbn.be/files/news/link/Advies_2016_22_Bewaring_boeken_en_verantwoordingsstukken_FR.pdf

- Conrad, D. (2016). *Enfin une vraie définition de la digitalisation*. Consulté le 2 Mai 2017, sur LinkedIn: https://fr.linkedin.com/pulse/enfin-une-vraie-d%C3%A9finition-de-la-digitalisation-dorian-conrad

- Coppens, P.-F. (2014). *Aspects fiscaux relatifs à la rectification du bilan - La notion d'erreur matérielle du bilan.* Consulté le 2 Mai 2017, sur IEC: https://www.iec-iab.be/fr/membres/publication/accountancy-tax/Documents/2014/05_A_T_2014_2_Rectification_du_bilan_Aspects_fiscaux.pdf

- De Leus, K. (2017). Il faut adapter la législation à la nouvelle réalité numérique. *L'Echo*.

- European Commission. (2017). *Assiette commune consolidée pour l'impôt des sociétés*. Consulté le 5 Mai 2017, sur European Commission: https://ec.europa.eu/taxation_customs/business/company-tax/common-consolidated-corporate-tax-base-ccctb_fr

- Ford, M. (2015). *The rise of the robots.* Etats-Unis: Basic Books.

- Gobert, D. (2016). *Archivage électronique : la loi belge complétant le règlement eIDAS est publiée ce jour*. Consulté le 9 Avril 2017, sur Droit & Technologies: https://www.droit-technologie.org/actualites/archivage-electronique-la-loi-belge-completant-le-reglement-eidas-est-publiee-ce-jour/

- Gonzalez, E. (2016). *Digitalisation d'entreprise concrètement, que faut-il transformer ?* Consulté le 24 Avril 2017, sur Monde Economique: https://www.monde-economique.ch/fr/posts/view/digitalisation-d-entreprise-concretement-que-faut-il-transformer

- Gryson, E. (2017, 27 Avril). Interview du CEO de Ricoh Belgium SA. [Entretien]. Bruxelles.

- ICCI. (2017). *Séminaire - Contrôle IT dans un contexte ISA : nouvelle technologie, nouveaux risques d'audit + Information Produced by the Entity (IPE)*. Bruxelles.

- IPCF. (2008). *T.V.A. – mentions obligatoires des factures.* Consulté le 24 Avril 2017, sur IPCF: http://www.ipcf.be/Uploads/Documents/doc_1704.pdf

- ISACA. (2013). *Norme d'audit et d'assurance des SI 1201 - Planification de la mission.* Consulté le 20 Novembre 2016, sur ISACA: http://www.isaca.org/Knowledge-center/Standards/Documents/1201_std_French_1113.pdf

- ISACA. (2013). *Norme d'audit et d'assurance des SI 1202 — Évaluation du risque dans la planification.* Consulté le 19 Novembre 2016, sur ISACA: https://www.isaca.org/Knowledge-Center/Standards/Documents/1202_std_French_1113.pdf

- ISACA. (2013). *Norme d'audit et d'assurance des SI 1207 - Irrégularités et actes illégaux.* Consulté le 19 Novembre 2016, sur ISACA: https://www.isaca.org/Knowledge-Center/Standards/Documents/1207_std_French_1113.pdf

- ISO. (s.d.). *Organisation internationale de normalisation*. Consulté le 12 Avril 2017, sur ISO: https://www.iso.org/fr/about-us.html

- Marché Public. (2013). *Système informatique*. Consulté le 30 Avril 2017, sur Marché Public: http://www.marche-public.fr/Terminologie/Entrees/systeme-informatique.htm

- MBD Consulting. (2016). *Digitalisation d'entreprise - La Stratégie à l'ère du digital*. Consulté le 3 Mars 2017, sur MBD Consulting: http://mbdconsulting.ch/fr/blog/strategie/digitalisation-dentreprise-la-strategie-lere-du-digital/#.WSHNgBLyh-U

- Nifccanada. (2009). *Norme ISA 265, Communication des déficiences du contrôle interne aux responsables de la gouvernance et à la direction.* Consulté le 13 Novembre 2016, sur Normes d'information financière et de certification Canada: http://www.nifccanada.ca/key-terms-french-only/item34648.pdf

- Nifccanada. (2012). *Norme ISA 315 (révisée), Compréhension de l'entité et de son environnement aux fins de l'identification et de l'évaluation des risques d'anomalies significatives.* Consulté le 13 Novembre 2016, sur Normes d'information financière et

de certification Canada: http://www.nifccanada.ca/key-terms-french-only/item21189.pdf

- PWC. (2017). *Carrières France - L'auditeur*. Consulté le 17 Avril 2017, sur PWC: http://carrieres.pwc.fr/fr/explorer-nos-metiers/auditeur.html

- Reputation VIP. (2017). *Les risques de l'e reputation pour une entreprise*. Consulté le 29 Avril 2017, sur Reputation VIP: https://www.reputationvip.com/fr/guide/risques/pour-entreprise

- SPF Economie, P. C. (2016). *Baromètre de la société de l'information 2016.* Consulté le 25 Janvier 2017, sur SPF Economie, P.M.E., Classes moyennes et Energie: http://statbel.fgov.be/fr/modules/publications/statistiques/marche_du_travail_et_conditions_de_vie/barometre_de_la_societe_de_l_information_2016.jsp

- SPF Economie – DG Statistique – Statistics Belgium, Eurostat (2015). Enquête 'Utilisation des TIC et de l'e-commerce dans les entreprises'. Récupéré le 25 Janvier 2017 de http://statbel.fgov.be/fr/binaries/Barometre_de_la_societe_de_l_information_2016_tcm326-278973.pdf

- Université Grenoble Alpes. (2017). *Politique de Sécurité du Système d'Information (PSSI)*. Consulté le 15 Avril 2017, sur Université Grenoble Alpes: https://services-numeriques.univ-grenoble-alpes.fr/catalogue-services/securite/politique-securite-systeme-information-pssi

- Valero, J. (2016). *La justice européenne appelée à trancher sur le statut d'Uber*. Consulté le 25 Avril 2017, sur Euractiv: http://www.euractiv.fr/section/euro-finances/news/uber-gains-key-support-from-member-states-before-eu-court-hearing/

- Van Aerssen, X. (2017, 20 Avril). Interview du gérant du cabinet comptable SPRL Excellium Solution. [Entretien]. Bruxelles

- Wooxo. (s.d.). *Notre métier - Editeur français de solutions de protection et de management documentaire.* Consulté le 1 Mai 2017, sur Wooxo: http://www.wooxo.fr/connaitre-wooxo/metier

- Yolin, J. M. (2009). *Les TIC : des outils incontournables pour les entreprises*. Consulté le 2 Mai 2017, sur Agence France Entrepreneur: https://www.afecreation.fr/cid94702/les-tic-des-outils-incontournables-pour-les-entreprises.html?&pid=326