h e g

Haute école de gestion
Genève

Gestion des risques informationnels dans les organisations

Mémoire de recherche réalisé par :

Giselle CASTELO BRANCO

Monika BOLLIGER

Sous la direction de :

Basma MAKHLOUF SHABOU, professeure HES

Genève, 17 janvier 2018

Master en Sciences de l'information

Haute École de Gestion de Genève (HEG-GE)

Hes·so GENÈVE
Haute Ecole Spécialisée de Suisse occidentale

Déclaration

Ce travail de Master est réalisé dans le cadre du Master en Sciences de l'information de la Haute école de gestion de Genève. L'étudiant accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans ce travail, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteur/des auteurs, ni celle de l'encadrant.

«J'atteste/Nous attestons avoir réalisé le présent travail sans avoir utilisé des sources autres que celles citées dans la bibliographie. »

Fait à Genève, le 17 janvier 2018.

Giselle Castelo Branco

Monika Bolliger

Remerciements

Nous tenons à remercier les personnes qui ont contribué à la réalisation de ce projet de recherche.

Notre directrice de mémoire, Mme Makhlouf-Shabou, professeure à la HEG et son assistant Aurèle Nicolet pour le temps qu'ils nous ont consacré.

Les participants aux interviews dans les diverses institutions. Nous ne les nommerons pas, car ils ont souhaité rester anonymes. Mais nous aimerions les remercier de nous avoir reçu avec autant d'égards, d'avoir passé plusieurs heures à étudier nos questions et de s'être beaucoup investis pour répondre au mieux à nos nombreuses questions.

Nos collègues et amis pour les conseils.

Nos familles pour leur patience et appui.

Résumé

L’usage de technologies et médias dans les sociétés modernes ont mis sur le devant de la scène les risques techniques, informatiques et plus récemment les risques informationnels. L’information et le patrimoine informationnel constituent une vraie richesse pour l’entreprise. Mais l'information circule, se partage et plus elle est partagée, plus elle risque d’être malmenée. La gestion des risques informationnels, la sécurité de l'information, font l’objet de plus en plus d'études au vu des conséquences que peuvent avoir la fuite, le vol ou la divulgation d’informations importantes.

Notre démarche est exploratoire. La première étape était de parcourir la littérature et de faire un état de l’art des risques informationnels, puis de comparer la littérature à la réalité sur le terrain par des interviews dans les milieux professionnels en Suisse romande.

La recension des écrits a révélé que ces risques apparaissent dans les ouvrages sur la gestion des risques, la sécurité informationnelle ou des SI, la protection de l'information ou du patrimoine informationnel, dans le domaine de la gouvernance de l’information, en archivistique et en intelligence économique.

Dans la gestion des risques, le risque informationnel occupe encore une place marginale que ce soit dans la littérature ou sur le terrain. Il s'efface derrière d’autres risques. C’est au niveau de l'identification du risque qu'il faut prendre conscience de son existence et de son importance. S’il est identifié, sa gestion n'est, à priori, pas problématique, car la gestion des risques est bien documentée et réglée par des normes et des professionnels du risque. Nous disons « à priori », car la gestion des risques n’est pas faite que de tableaux d’évaluations, d’analyses et de traitements de risques. La gestion implique aussi la définition de tâches, de responsabilités.

L’analyse des résultats montre que la gestion du risque informationnel n’est attribuée à personne en particulier, qu’elle relève de beaucoup d’acteurs : des gestionnaires de risques, des archivistes, des responsables SI et est traitée de façon segmentée. Or, si l’information circule dans tous les secteurs et est de nature transversale, elle demanderait une gestion elle aussi transversale, qui puisse l’accompagner dans ses flux et ses cycles.

L’objectif final de ce travail étant de proposer un modèle de gestion des risques informationnels et ses composantes, nous avons choisi de proposer une gestion centralisée de tous les actifs informationnels de l’entreprise en partant des objectifs préalablement définis par les différents acteurs de l’institution. Ceux-ci seraient représentés de façon égale dans un nouveau département qui serait créé à ces fins et rattaché à la direction.

Mots-clefs :

Gouvernance de l’information - risque informationnel - sécurité de l’information - gestion des risques - entreprise - gestion transversale des risques - Suisse romande

Table des matières

Liste des figures

Sigles et abréviations

B : Banque

BDD : Base de données

DS : Département de sécurité cantonal

DSI : Direction des systèmes d'information

GRI : Gestion des risques informationnels

HOP : Hôpital cantonal

IRE : Institut de recherche et d'enseignement

OI : Organisation Internationale

PME : Petite et moyenne entreprise

RI : Risque informationnel

RSSI : Responsable de la sécurité du système d'information

SI : Système d'information

TI : Technologies de l'information

VPN : Virtual Private Network

1. Introduction

Les termes employés pour désigner des personnes dans ce travail sont pris au sens générique, ils ont à la fois valeur d'un féminin et d'un masculin.

1.1 Problématique

« De plus en plus confrontées aux problématiques de risques, les entreprises sont progressivement devenues sensibles à la nécessité d'une gestion efficace des risques » (Lacroix 2007, p.6). Mais les risques sont de diverses natures. Dans ce travail nous nous intéressons au risque informationnel. L'information, qui fait l'objet de beaucoup d'attention aujourd'hui, est-elle fiable, est-elle maîtrisée ? Toute organisation produit de l'information, celle-ci circule partout que ce soit de manière formelle ou informelle, elle est techniquement protégée et contrôlée pour en limiter l'accès ou alors expressément divulguée pour des soucis liés à la transparence ou à la réputation. L'information a de la valeur et sa gestion demande des efforts de temps et d'argent. Avec le développement technologique et la variété des supports, le flux d'échange informationnel s'est accru au point qu'il n'est pas évident de tout contrôler. Comment se prévenir, par exemple, des risques liés à une fuite d'informations ou de la perte de données enregistrées ? Comment protéger l'information si, en même temps, il est nécessaire de la partager et de la rendre accessible ? Les risques sont nombreux et les conséquences peuvent être plus ou moins graves pour l'entreprise. Il n'est qu'à citer le vol des données de 1.3 millions de clients d'Orange en 2014[1] ou le vol des informations confidentielles relatives à des employés et des films inédits de Sony Pictures[2] cette même année.

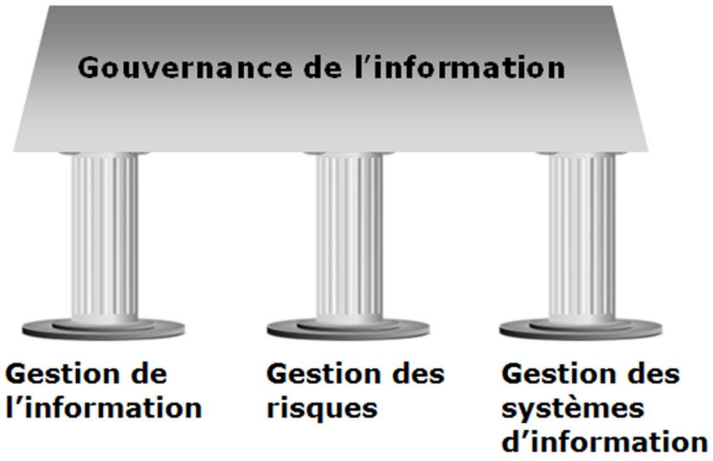
Quelles sont les conséquences pour une entreprise si l'information qui constitue l'essence même de ses activités n'est pas bien gérée ou n'est pas sécurisée ? Qui serait touché ? La bonne gestion de l'information et des risques qui lui sont liés assure la performance, la crédibilité et la réputation d'une entreprise.

> *« Les préjudices subis par les entreprises victimes incluent évidemment le coût économique direct, mais les pertes de données et d'informations confidentielles entraînent également des répercussions négatives sur la réputation de l'organisation, un gaspillage de ressources affectées au rétablissement des systèmes et à la reconstitution des données, la perte de clients et de fournisseurs, ainsi que l'imposition d'amendes par les autorités réglementaires ». (Hejazi et Lefort 2009, cité dans Asseman et Dupont 2011, p.5)*

Cette problématique si actuelle relève de la gestion du risque informationnel. Pour situer ce dernier dans la structure managériale d'une entreprise, nous nous sommes basées sur les études en gouvernance de l'information (GI). Au même titre que le management de l'information et la gouvernance des systèmes d'information (IT), la gestion des risques informationnels fait partie des composantes de la GI (Hagmann, Burgwinkel et Wildhaber 2016).

[1] Belouezzane, Sarah, 2014. Orange de nouveau victime d'une cyberattaque massive. *Le Monde : Economie* [en ligne]. 07 mai 2014.
[2] Boy, Louis, 2014. Les révélations embarrassantes du piratage de Sony Pictures. *France Info : Culture* [en ligne] 04 décembre 2014.

Figure 1 : Principes de la gouvernance de l'information



(Inspiré de Hagmann, Burgwinkel et Wildhaber 2016, chapitre 2.4.3)

> *« IG is a subset of corporate governance, and includes key concepts from records management, content management, IT and data governance, information security, data privacy, risk management, litigation readiness, regulatory compliance, long term digital preservation, and even business intelligence. »* (Smallwood 2014, p.5)

1.2 Définitions

1.2.1 Risque

Nous partirons de la définition du risque présentée dans le Petit Robert et citée par Lacroix (2007, p.9) :

> *« [Le risque est l']éventualité d'un événement ne dépendant pas exclusivement des parties et pouvant causer la perte d'un objet ou tout autre dommage ; par extension, [le risque est un] événement contre la survenance duquel on s'assure. »*

1.2.2 Information et donnée

Les termes « information » et « donnée » seront utilisés comme suggéré par Banat-Berger, Duplouy et Huc :

> *« L'information est définie comme une connaissance qui peut être échangée. L'information est généralement perçue par l'intermédiaire d'un capteur qui transmet un signal [...] Lorsque l'information a été captée, elle pourra être mémorisée [...] »* (Banat-Berger, Duplouy et Huc 2009, p.21)
>
> *« La donnée est définie comme un conteneur porteur d'une information. La donnée est une représentation formalisée de l'information. Un texte, une image, un graphique sont des données supports d'information. »* (Banat-Berger, Duplouy et Huc 2009, p.21)

1.2.3 Patrimoine informationnel

> *« Le patrimoine informationnel peut être considéré comme l'ensemble des données et des connaissances, protégées ou non, valorisables ou historiques d'une personne physique ou morale. » (Caprioli 2007, p.8)*

Desroches (2013, p.12-13) cite cette définition et reprend les éléments qui peuvent composer le patrimoine informationnel à Morizot (cité par Desroches, p.13) : le savoir-faire de l'entreprise, les informations commerciales, les informations sur le personnel de l'entreprise, les partenaires de l'entreprise, les informations financières et les informations juridiques. Elle

ajoute que « l'information doit être considérée à travers deux types d'actifs : le patrimoine immatériel [...] et le patrimoine matériel [...] ».

1.2.4 Actif informationnel

Les actifs informationnels sont les « assets » en anglais. Ce terme est souvent utilisé comme un synonyme de « patrimoine informationnel ». Selon Vallès, « les actifs informationnels touchent tous les éléments rentrant dans le processus de mise en place et d'exploitation des systèmes d'information de l'entreprise. Cela prend en compte le matériel informatique, les processus, les données, de même que l'information conservée sur support papier ou sur tout autre type de support » (Vallès 2015, p.4).

Les termes « organisme », « organisation », « société » et « institution » seront utilisés de manière interchangeable. Nous ne nous référerons spécifiquement à l'un des groupes mentionnés que si cela est nécessaire.

1.3 But et objectifs de la recherche

Le but de ce travail est d'établir un état de l'art des risques informationnels en se basant sur la littérature récente et en comparant celle-ci à la réalité sur le terrain.

Ce travail a trois objectifs :

1- Définir et identifier le risque informationnel.

2- Lister les moyens employés par les organismes pour la gestion des risques informationnels.

3- Proposer un modèle de gestion des risques et faire des recommandations.

1.4 Questions de recherche

Nos questions de recherche sont les suivantes :

- Quelle est la définition de « risque » ? Et celle de « risque informationnel » ?
- Quels sont les types de risques informationnels listés par la littérature ?
- Comment les risques informationnels sont-ils évalués ?
- Comment sont-ils traités ? Quels outils ou logiciels sont utilisés pour leur traitement ?
- Quelles normes et lois sont directement liées au risque informationnel ?
- Qui a la responsabilité de ce type de risque dans l'entreprise ?

C'est-à-dire, comment le RI est-il appréhendé, identifié, défini, traité, quelle place il occupe parmi les autres risques et qui les gère ?

2. Revue de la littérature

2.1 Introduction

La recension des écrits suit les points de la grille de lecture établie en fonction des objectifs de la recherche. Nous avons trouvé pertinent d'insérer une partie dédiée à l'information, thème central de ce travail.

2.2 L'information

Qui dit identifier des risques, dit aussi mettre en marche une politique fonctionnelle pour leur gestion puisque les enjeux peuvent coûter la survie de l'entreprise : « L'information est à la fois une matière première vitale et aussi une source de menaces fortes pour toute organisation », lit-on dans le livre blanc de l'Observatoire de la gouvernance de l'information et 3ORG conseil (2012). Les actifs informationnels ou le patrimoine informationnel varient d'une organisation à l'autre. Les types de risques sont nombreux et la perception des risques est subjective. La gestion ou le management de ces derniers relèvent donc d'approches multiples. Pour prendre en compte les risques liés à l'information, il faudrait encore penser à tout ce qu'elle implique :

> *« L'information est un objet très complexe. Non seulement elle porte un contenu, mais on lui associe aussi une forme, un poids, des droits d'accès, des dépendances techniques et surtout un contexte. Elle a par ailleurs une valeur, un coût, une criticité, une intégrité, voire une disponibilité plus ou moins forte selon l'étape de son cycle de vie. »* (Observatoire de la gouvernance de l'information et 3ORG conseil 2012, p.17))

2.2.1 L'information dans l'entreprise

Etant donné son caractère fluide et changeant, nous estimons qu'il est difficile de classer l'information dans une seule catégorie. Souvent elle fait partie de plusieurs catégories à la fois. Pour cette raison, nous avons choisi de travailler avec la classification de Lesca (2010, p.17), qui le fait selon sa finalité en entreprise. Certes, il s'agit encore une fois d'essayer de mettre un concept très fluide dans des cases, mais son raisonnement nous semble le plus adapté pour aborder la protection de l'information en entreprise dans ce travail :

- **Information de fonctionnement :** « Ensemble des informations qui sont (à peu près) indispensables au fonctionnement « mécanique » quotidien de l'entreprise (…). Sans ces informations, les tâches courantes de l'entreprise ne pourraient pas être réalisées et contrôlées. La production de ces informations est continue. » Exemples : Les commandes client et fournisseur, la fiche de stock, bilans, fiches de paie, etc.
- **Information d'influence :** « La finalité est d'influer sur le comportement des acteurs pertinents pour l'entreprise, que ces acteurs soient internes (le personnel) ou externes (clients, concurrents…), afin de les rendre aussi « coopérants » que possible » (...) L'influence peut être exercée vis-à-vis de l'intérieur de l'entreprise (ou organisme), et/ou vis-à-vis de l'extérieur. Mais l'inverse existe aussi : l'influence exercée, par les acteurs extérieurs, sur l'entreprise. » Exemples : bruits de couloirs, communication interne, publicité, sponsoring, catalogue de produits, etc.
- **Information d'anticipation :** « Permet à l'entreprise de voir venir à l'avance certains changements de son environnement socio-économique dans le but d'en tirer un avantage ou bien d'éviter un risque. » Exemples : veilles économique, stratégique, législative, scientifique, etc.

2.3 Définition de risque

Le terme de risque est largement défini dans la littérature, car il a diverses acceptions. C'est un mot vénitien d'origine espagnole (riesgo) ou un mot italien (risco) qui signifie rocher escarpé ou écueil (Bouzon 2001 et Léger 2013). Il est « utilisé [au XIVe siècle] pour désigner le péril couru en mer lors de l'apparition des premières compagnies d'assurances [maritimes en Italie] » , dit Léger (2015a, p.3).

Kermisch (2012) consacre un article à la définition du risque et relève, par exemple, que le risque n'existe pas sur le plan ontologique, qu'il n'est que virtuel ou potentiel. Matérialisé, il ne s'agit plus de risque, mais de sinistre. « Tout risque se caractérise [par ailleurs] par un coût, lié entre autres à l'obligation de le « provisionner », c'est-à-dire de se préparer à son impact financier au cas où il se concrétiserait », nous dit le Groupe Société Générale (2017, p.1).

Il faut ajouter que le risque peut aussi avoir des conséquences positives et être considéré comme opportunité. Mareschal, par exemple, dit que « le risque est un mélange de trois notions : aléas, dommage et opportunité [...] » (Mareschal 2003, p.7-8). Le risque positif est aussi pris en considération dans l'ISO 31000:2009 : « Le risque est un effet de l'incertitude sur l'atteinte des objectifs » et l'effet est « un écart positif et/ou négatif par rapport à une attente ». Il y a différence entre les attentes et la réalité. Lemieux et Krumwied disent que la prise de risque est souvent perçue comme positive dans le domaine financier, car il n'y a pas de profit sans prise de risque (Lemieux et Krumwied 2011). Seul Léger estime que le risque positif n'est pas à mitiger, qu'il est accueilli favorablement et parle alors de possibilités. « La gestion des possibilités positives n'est pas de la gestion de risque », dit-il (Léger 2013, p.26).

Léger a recensé de nombreuses définitions du risque sur son site et souligne que « le risque est un construit social qui dépend de celui qui le perçoit, de la nature du risque et du domaine dans lequel on s'intéresse au risque » (Léger 2013, p.23). Trois points sont ici à relever : La perception du risque qui est subjective et qui pourrait peut-être être davantage gérée que le risque lui-même (Bouzon 2001), la nature du risque dont on parlera dans l'identification des risques et le domaine qui traite des risques. Pierandrei (2015) dit à propos de ce dernier point que le terme « risque » est complexe et prend différents sens suivant le domaine d'étude : mathématique, économie, finance, psychologie, neurosciences ou science de l'ingénieur. Il est aussi perçu et traité différemment selon ces disciplines.

Dans notre domaine, celui de l'économie, le risque est étroitement associé à la protection des valeurs ou actifs d'une organisation ou d'une entreprise. Le baromètre du Risk management 2011 de Protiviti recommande d'adopter une définition large du risque, car chaque entreprise doit pouvoir identifier rapidement les risques auxquels elle est confrontée. Il est écrit que « le risque correspond à toute incertitude ou tout événement pouvant menacer les activités et les actifs de l'entreprise et ainsi entraver l'atteinte de ses objectifs et son développement à long terme » (Protiviti 2011, p.8). Léger dit que le risque n'est pas l'incertitude. Celle-ci ne se gère pas et ne s'exprime pas par des probabilités (Léger 2013, p.24-26).

Beaucoup de définitions reprises entre autres par Lacroix (2007), le Clusif (Club de la sécurité de l'information français, 2009), Léger (2013 et 2015a), Vallès (2015) ou Lemieux (2004a) présentent le risque par rapport aux notions de menaces, vulnérabilités, probabilités, occurrences et conséquences. Ce sont les éléments constitutifs des risques.

Vallès dit que « le risque est la probabilité qu'un effet spécifique se produise dans une période donnée ou dans des circonstances déterminées. En conséquence, un risque se caractérise par deux composantes : la probabilité d'occurrence d'un événement donné ; la gravité des effets ou des conséquences de l'événement supposé pouvoir se produire » (Vallès 2015, p.3).

Lemieux relève des points essentiels sur la définition des risques : « Risk is a description of a thing, event or action that has not yet occurred ; that thing, event or action has a certain probability of occurring ; a risk has a consequence or impact after it has occurred ; determination of probability and impact requires making assumptions about the future ; risk is a relative concept : assumptions about the future need to be made within an organisational context ; risk can be managed » (Lemieux 2004a, p.8-10).

Le Clusif (2009) part aussi de la protection des valeurs ou actifs des organisations pour définir le risque. Il tient compte des menaces ou actions qui peuvent nuire à ces actifs en tenant compte des éventuelles vulnérabilités (niveau d'exposition au risque). Comme cette vision du risque est statique et ne prend pas en considération la variable « temps » et l'enchaînement d'événements ou de causes et conséquences, le Clusif propose aussi une définition du risque par scénario. Il s'agit de descriptions de situations de risque. Le risque est la conjonction d'un actif, d'un type de dommage pouvant être subi par cet actif et de circonstances dans lesquelles ce dommage pourrait survenir (Clusif 2009). Cette vision du risque se veut dynamique.

Enfin, le risque doit être contextualisé, il doit être évalué et traité afin qu'une société puisse préserver ses actifs et atteindre ses objectifs. Ses définitions devraient contenir les termes de contexte, actifs, perception, objectifs en plus des éléments constitutifs du risque, notamment la conséquence plutôt négative.

2.4 Définition du risque informationnel

Hassid présente l'évolution des risques des années 1970 à 2000. Il place le risque informationnel en dernier et le lie à l'arrivée des nouvelles technologies dans les années 1990 et à l'importance que prennent les médias dans les entreprises. Il ne le définit pas, mais dit que « ce n'est pas un risque neutre, il a tendance à se combiner avec les autres risques […] » (Hassid 2008, p.24).

Le risque informationnel n'est effectivement pas toujours reconnu comme un type de risque en soi et il apparaît donc de manière discrète ou indirecte dans la littérature ou les baromètres des risques. On le retrouve par exemple parmi les risques de la gestion de la connaissance (Darsa 2013) et plus régulièrement parmi les risques IT qui font partie des risques opérationnels (Lacroix 2007) ou risques internes (Protiviti 2011), etc. Il occupe une place plus importante en intelligence économique (Ecole Européenne d'intelligence économique 2011), dans les écrits sur la protection de l'information, du système d'information ou du patrimoine informationnel. Il apparaît aussi dans les textes juridiques relatifs à la sécurité des biens immatériels et il est également cité dans les écrits sur la gouvernance de l'information et en archivistique/records management.

Actuellement, il existe une définition du risque informationnel dans le domaine de l'intelligence économique. Elle nous est donnée par Harbulot : **«** Le risque informationnel est la manifestation d'une information, avérée ou non, susceptible de modifier ou d'influencer l'image, le comportement ou la stratégie d'un acteur. Son impact peut se traduire par des pertes financières, technologiques ou commerciales » (Harbulot 2005). On peut compléter ces

propos par ceux de Huyghe ([s.d.]) : « le risque naît de et par l'information. Il se manifeste quotidiennement à travers la vulnérabilité des réseaux et des systèmes, par le péril de réputation, par la désinformation ou la mésinformation, par des affaires de secrets violés, par la déstabilisation ou le pilori médiatique ».

Dans les autres domaines, le risque informationnel cherche encore un peu sa définition. Nous citerons celle de Léger et Vallès : « le risque informationnel est celui associé à la sélection, la mise en forme, le transfert et l'utilisation de l'information » (Léger 2013, p. 30 ; Vallès 2015, p.3). Léger dit au début de son « introduction à la gestion de risque informationnel » : « ce livre porte sur la gestion du risque informationnel, c'est-à-dire sur la gestion des risques associés à la gestion des informations dans les organisations » (Léger 2013, p.6).

Il y a donc des risques liés à la gestion de l'information, mais il y a aussi des risques liés à l'information en général. Pour définir le risque informationnel, regardons ce qu'on entend par information, vu que c'est un risque relatif à l'information. Nous en avons déjà donné quelques caractéristiques, mais on peut ajouter d'autres éléments ou sources intéressantes qui sont davantage en relation avec le sujet traité ici.

Dans l'économie de l'immatériel, pour reprendre les termes de Moinet, l'information s'apparente à la communication. Elle circule, elle est souvent mise en forme rapidement et elle est périssable ; « le flux prime sur le stock » (Moinet 2014, p.46). On se demande alors s'il est plus avantageux de diffuser ou de protéger l'information. « L'information a un prix », elle est parfois secrète et « donne un pouvoir à celui qui la détient, mais ce pouvoir est provisoire » (Moinet 2014, p.46). Dans le résumé d'une des conférences de Harbulot, « [il est question] d'attaques informationnelles qui peuvent prendre différentes formes : créer un doute sur la qualité des produits d'une entreprise, nuire à la réputation de ces dirigeants ou encore de diffuser des rumeurs sur les résultats financiers ou commerciaux » (Harbulot 2005). On se rapproche ici d'un autre risque, celui de réputation ou d'image. Du Manoir de Juaye parle de la difficulté de se protéger contre le cyberharcèlement. Les attaques ou rumeurs ne durent souvent qu'un mois et les procédures judiciaires sont longues et ne font souvent que les envenimer. Il est aussi difficile d'identifier les médias qui diffusent la « fausse » information (Du Manoir de Juaye 2014).

Pour Perrein, spécialiste en gouvernance de l'information, l'information a une valeur, un coût ; il s'agit de la valoriser et de la maîtriser. C'est une source de menaces fortes pour toute organisation : fuite d'information, perte d'information, impossibilité de contrôler ou de restreindre ce qui se fait sur l'information, réputation, non-respect de la réglementation, présence d'information préjudiciable, information erronée, non traçabilité, etc. ». (Perrein 2012).

La valeur de l'information est aussi soulignée à l'Uniris, le service des ressources informationnelles de l'Unil : « l'information est un bien commun, une ressource stratégique faisant partie de la culture de l'institution. C'est une richesse à partir du moment où elle est correctement gérée, exploitable et transformée en connaissance » (Uniris 2016, p.5).

Pour Desroches (2013), l'information est blanche (accessible à tous), grise (accès restreint) ou noire (inaccessible). L'information est l'ensemble des données, des connaissances, du savoir-faire propre d'une entreprise. De l'information, on est passé au patrimoine informationnel. Vallès parle, lui, d'actifs informationnels. Pour lui, « le risque informationnel est

associé au processus de traitement de l'information, traitement qui prend place comme composante du système d'information » (Vallès 2015, p.4).

Les données informationnelles, les actifs informationnels sont de plus en plus protégés par la loi. Vermeys (2009) parle de leur sécurité : « en matière informationnelle, la sécurité peut être définie comme étant la protection des ressources informationnelles d'une organisation, face à des risques identifiés, qui résulte d'un ensemble de mesures de sécurité prises pour assurer la confidentialité, l'intégrité et la disponibilité de l'information traitée. La sécurité informationnelle doit donc être perçue comme étant la sécurité de l'information et non de l'informatique ». On vise le contenu et non le support (Vermeys 2009, p.4-5).

Le risque informationnel est donc lié à une information, une donnée, une rumeur ou aux actifs informationnels. Le risque peut venir de l'information, du traitement ou de la diffusion de l'information. Mais un événement ou risque peut aussi impacter, avoir des conséquences négatives sur l'information ou les actifs informationnels. Léger dans sa typologie des risques informationnels classe les risques selon qu'ils occasionnent des dommages matériels ou immatériels. Il nous donne l'exemple d'une erreur humaine, d'une mauvaise manipulation qui peut causer la perte d'un fichier (Léger 2015b). Vallès dit aussi que « le risque informationnel prend en compte les menaces auxquelles sont exposés les actifs informationnels de l'entreprise » (Vallès 2015, p.4).

Les deux cas de figure apparaissent dans l'article de l'avocat Du Manoir de Juaye (2014) qui cite les deux grandes catégories de risques informationnels actuels : il y a « celle qui concerne le risque de voir une information appréhendée contre la volonté de son détenteur et celle concernant la diffusion de fausses informations, d'informations mensongères de manière volontaire ou non » (Du Manoir de Juaye 2014, p. 37). L'ensemble des acteurs qui manipulent le patrimoine doivent être sensibilisés à la protection de l'information et ne pas faire courir de risques à l'entreprise. Un article de Deleporte et Sfez (2013) présente un certain nombre de comportements à risque qui causent des pertes, divulgations ou vols de données confidentielles, puis énumère les bonnes pratiques qui protègent la richesse informationnelle d'une entreprise.

Donc si l'on revient à la définition du risque informationnel, celui-ci semble avoir deux sens. Soit l'information est porteuse de risques ou est source de risques, soit un risque impacte ou a des conséquences fâcheuses sur l'information ou les actifs informationnels. Les deux sont représentés dans les articles juridiques. Les catégories de risques informationnels que nous verrons au chapitre suivant reposent en partie sur cette dualité « cause et/ou conséquence de risques ». On ajoutera que l'un n'exclut pas l'autre. L'Uniris, le service des ressources informationnelles de l'Unil, mentionne qu'une bonne gestion de l'information permet de maîtriser, par exemple, les risques juridiques comme la non-conservation d'information à valeur probante (Uniris 2016). On pourrait aussi dire que la non-conservation d'information à valeur probante est un risque informationnel. Et la mauvaise gestion de l'information constitue aussi un risque informationnel. On constate déjà ici que la catégorisation des risques a ses limites et explique aussi l'effacement du risque informationnel derrière les autres types de risque ; cela rejoint la combinaison des risques qu'évoquait Hassid (2008). Une définition du risque informationnel devrait donc englober ces deux aspects. Celle de Léger et Vallès, ci-dessus, va dans le bon sens, car elle est assez globale : « le risque informationnel est celui

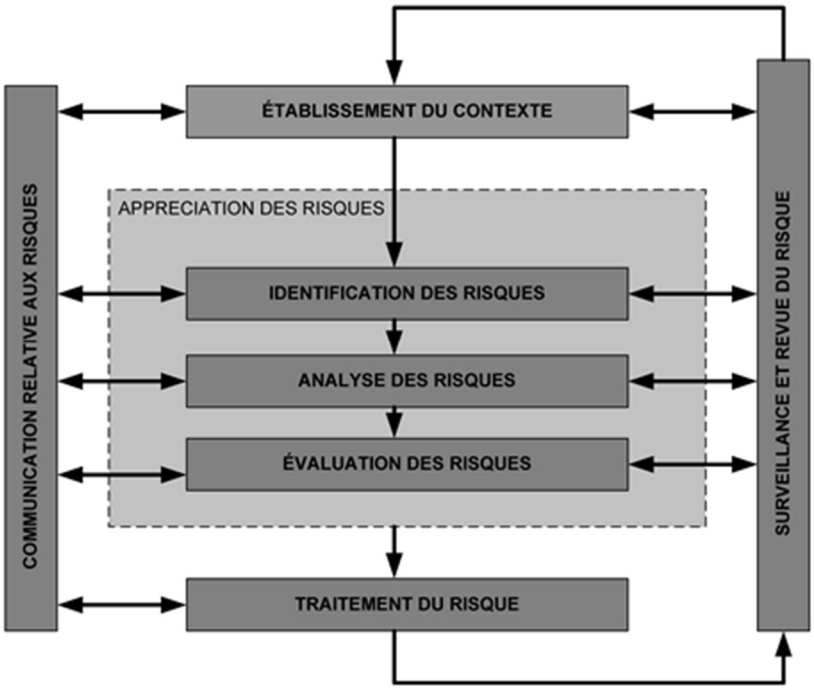
associé à la sélection, la mise en forme, le transfert et l'utilisation de l'information » (Léger 2013, p.30 ; Vallès 2015, p.3).

2.5 Gestion des risques

La gestion des risques informationnels vise à assurer que la disponibilité, l'intégrité et la confidentialité des données ne soient pas compromises. Ce sont là les trois principes de la sécurité informationnelle (Vermeys 2009)[3]. On identifie et évalue les risques pour pouvoir les maîtriser, les réduire ou les gérer au mieux. Certains parlent de management de risques, d'autres de gestion, d'évaluation de risques ou même de processus de la gestion des risques. Le tableau ci-dessous présente la gestion des risques de la norme ISO 27005:2011. Lemieux (2004a) a une version similaire dans son « risk management », qui présente : « l'analyse du contexte (contextual analysis), l'identification des risques (risk identification), la description des risques (risk description), l'évaluation des risques (risk assessment), le traitement des risques (risk treatment), le contrôle du risque, le monitoring ou l'audit (risk monitoring and control) » (Lemieux 2004a). Il y a d'autres variantes dans ces étapes. La plupart des auteurs ont l'identification, l'analyse et le traitement des risques. Le Clusif (2009) ne met, par exemple, pas le contrôle, mais parle de la communication des risques à la fin, etc. Darsa analyse le contexte comme Lemieux. Il estime que c'est une étape importante, qu'il faut comprendre l'environnement de l'entreprise, ses métiers, son organisation, ses compétences, ses spécificités etc. pour identifier et évaluer ses risques (Darsa 2013, Lemieux 2004a). Pour évaluer le contexte, le portail PME de la Confédération suisse propose de faire une analyse des points forts et faibles (analyse SWOT) (DEFR 2017). Desroches (2013) relève les 3 étapes suivantes : la définition du contexte organisationnel, l'identification des risques et l'analyse des risques. Léger présente, lui, le processus IPM des risques : activité d'identification (I), d'évaluation de scénarios de risque avec aléas et vulnérabilités, priorisation des risques (P) et d'actions de mobilisation (M) (Léger 2013).

[3] Cette triade DIC (disponibilité-intégrité-confidentialité) est parfois complétée par la traçabilité, l'authenticité, la fiabilité, etc. Ces propriétés sont rejetées par Vermeys (2009, p.51-53), car elles se retrouveraient de manière implicite dans la triade de base.

Figure 2 : Processus de la gestion des risques



(ISO 27005 :2011, p. 8)

2.6 Types de risques informationnels

Les méthodes d'identification des risques sont variées. On peut se référer à des situations de risques passées ou à des retours d'expériences. Un certain nombre d'observatoires sont aussi apparus (Hassid 2008). On peut proposer des questionnaires auprès du personnel (par département, processus, etc.), « descendre » chercher l'information (approche top-down). L'identification des risques peut aussi se faire de manière plus ouverte par les personnes les plus proches des activités à l'aide d'interviews (approche bottom-up) (Mareschal 2003). « Les enquêtes aident à avoir une idée assez précise de la perception du risque que peuvent avoir les salariés et les consommateurs » (Hassid 2008, p.58). Darsa évoque encore d'autres indicateurs de risques, i.e. l'analyse de signes précurseurs (réclamations de diverses provenances, rapports, audits), la collecte et analyse de l'environnement extérieur (veille, presse), l'imagination, etc. (Darsa 2013).

Il est possible d'étudier l'ensemble des risques d'une société ou d'étudier des risques spécifiques à un domaine particulier, à des projets (Mareschal 2003, Clusif 2009).

Les entreprises et organisations classent souvent les risques par types, classes ou catégories pour qu'elles puissent les retrouver et les analyser plus facilement (cf. Eduscol 2015, Lacroix 2007, Lemieux, 2004, Darsa 2013).

Voici une liste de types de risques que l'on voit assez régulièrement dans la littérature :

- risque opérationnel et stratégique (Darsa 2013, Desjardins 2011, Marbaix 2016, Pierandrei 2015, ARMA International 2009, Lacroix 2007, Uniris 2016)
- risques internes / externes (Eduscol 2015, Protiviti 2011)
- risque financier (Darsa 2013, Marbaix 2016, Pierandrei 2015, ARMA International 2009, Lacroix 2007)

- risque juridique ou de conformité (Darsa 2013, Marbaix 2016, ARMA International 2009, Lacroix 2007, Uniris 2016)
- risque environnemental, climatique ou naturel (Marbaix 2016, ARMA International 2009)
- risque IT, SI, informatique ou technologique, cyberrisque (Darsa 2013, Marbaix 2016, Hassid 2008, Rouhier 2008)
- risque humain ou lié au RH (D.N. 2014, Marbaix 2016)
- risque politique, géopolitique (Darsa 2013, Hassid 2008)
- risque économique (Darsa 2013, Hassid 2008, Uniris 2016)
- risque de réputation ou d'image (Darsa 2013, Desjardins 2011, ARMA International 2009)
- risque informationnel (Hassid 2008, Lemieux 2004a et 2004b, Desroches 2013, Léger 2013 et 2017, Harbulot 2005, Marbaix 2016, Desjardins 2011, Ghernaouti-Hélie 2007, Moinet 2014, Du Manoir de Juaye 2014, Vallès 2015)

Regrouper les risques d'après leur provenance, nature ou domaine est avantageux dans la mesure où des personnes compétentes des milieux concernés peuvent contribuer à leur évaluation. D'autres regroupements, plus rares, existent (cf. Lemieux 2004a ; Lacroix 2007). Il faut ajouter que toute classification a ses limites et que les risques sont souvent interconnectés (Lemieux 2004a).

Le risque informationnel gagne en importance dans le monde actuel du numérique et de la communication. Il n'apparaît peut-être pas dans les listes de risques des ouvrages généraux, si ce n'est chez Hassid (2008), mais il fait l'objet de plusieurs études particulières (Lemieux, Desroches, Léger, Vallès, par ex.). Dans le milieu médical, on est de plus en plus confronté à ce risque dans la gestion des dossiers des patients (Harlow 2012) ou par rapport à l'information médicale diffusée sur le net (Vigouroux-Zugasti 2015). Dans le milieu bancaire, ce sont les données personnelles des clients que l'on s'efforce de protéger. « [Le groupe Desjardins relève] qu'un lien étroit semble s'établir entre le domaine de la protection des renseignements personnels et la gestion des risques informationnels » (Desjardins 2011, p.17).

Le risque informationnel se confond parfois aussi avec les risques informatiques, comme le montre l'article de Ghernaouti-Hélie (2007). Lemieux et Krumwied (2011) disent aussi que les risques informationnels sont souvent identifiés et classés parmi les risques opérationnels. Selon eux, ils seraient gérés plus efficacement s'ils étaient identifiés comme « records-related risks ».

Au sein de l'institution financière Desjardins, le risque informationnel ne constitue pas une catégorie de risque. Il est transversal, si l'on ose dire. L'information est au centre des activités, plusieurs unités sont impliquées dans la gestion de l'information (cf. ill. ci-dessous). Il faut avoir une vision globale des risques informationnels (Desjardins 2011).

Figure 3 : Gestion intégrée de l'information

(Desjardins 2011, p.19)

Regardons à présent quels types de risques se cachent derrière l'appellation « risque informationnel ». A dire vrai, il n'y a pas une liste précise de risques informationnels. Chacun propose sa manière d'identifier et classer les risques. Il n'y a pas d'unanimité. Nous allons résumer ce qui se dit.

Les auteurs ci-dessous présentent les risques informationnels que peuvent subir les documents et incluent souvent les risques informatiques. Pour eux, l'objectif de la gestion des risques informationnels est d'assurer la sécurité de l'information ou des actifs informationnels.

Vermeys (2009) regroupe en 7 catégories les risques à entrevoir en matière de sécurité informationnelle : dommage physique (vandalisme, panne, catastrophes naturelles), interaction humaine, défaillance technique, attaques internes, externes, abus de données (partage de secrets commerciaux, espionnage, vol), perte de données, erreurs logicielles.

Hassid (2008, p.23) reprend les 8 catégories de risques retenues par le cabinet Ernst & Young qu'il cite (pas de réf.) : l'utilisation de nouveaux outils ou techniques insuffisamment maîtrisés ; la dépendance de l'entreprise vis-à-vis de son système d'information ou de celui de ses partenaires ; des problématiques de sécurité informatique suite à l'interconnexion des réseaux et l'apparition d'internet ; la recrudescence de cas de malveillances et de fraudes informatiques ; une maîtrise et une maintenance des systèmes rendues difficiles par l'hétérogénéité et la complexité des technologies utilisées ; des difficultés à appréhender l'automatisation des processus opérationnels et la dématérialisation des échanges entre partenaires commerciaux; la mise en œuvre d'un « Entreprise resource planning » (ERP) sans véritable réorganisation des processus opérationnels ; le recours à la sous-traitance et l'externalisation de certaines parties des fonctions informatiques.

Pour Léger (2015) les principales catégories de risques sont la confidentialité, l'intégrité et la disponibilité des systèmes d'information. Il organise les risques informationnels en deux groupes : ceux qui causent des dommages matériels et ceux qui causent des dommages immatériels. Sont surtout mentionnés : la modification, la destruction ou la copie de données ; la non-disponibilité du SI ; l'accès non-autorisé des données.

Vallès (2015) reprend cette atteinte aux objectifs de sécurité de l'information et cite : la perte ou destruction de données ; la divulgation d'infos confidentielles ; la modification non autorisée des données ; la destruction, le sabotage ou vol d'actifs informationnels. Et il ajoute que « si ces risques se matérialisent, il en résultera pour l'entreprise des effets négatifs touchant le domaine financier, opérationnel, technique et légal de même que son image ou sa renommée » (Vallès 2015, p.4).

L'article d'Eduscol (2015, p.2) sur la Sécurité des systèmes d'information dit que les risques liés à l'information ont des caractéristiques propres. Leurs facteurs sont d'ordre :

- technologique : dysfonctionnement d'un composant pouvant perturber la fourniture d'un service, entraîner la perte de confidentialité d'une information ou nuire à l'intégrité du patrimoine informationnel de l'organisation
- humain : criminalité informatique, intrusion, espionnage industriel, erreurs humaines dans le choix ou l'usage d'une solution informatique
- risques naturels, essentiellement climatiques : chaleur/froid, inondations

Le Livre bleu des assises de la sécurité et des systèmes d'information propose aussi une typologie des risques informatiques et informationnels et rappelle que « les erreurs, inconsciences, négligences, voire parfois le stress ou les excès de confiance facilitent souvent l'acte malveillant » (Hapsis 2009, p.6) et cite le sabotage, l'intrusion, le vol, l'atteinte à la vie privée, la fraude, le piratage, les contenus illégaux.

D'autres comme l'Uniris (2016) mettent l'accent sur le records management et la gouvernance de l'information. Là, on ne parle pas de risques informationnels. La bonne gestion de l'information évite ou minimise les risques qualificatifs et juridiques, les risques stratégiques et les risques économiques. C'est la « mauvaise » gestion de l'information qui est source de risques. Sont mentionnés des exemples comme : la mauvaise gestion documentaire qui entraîne des problèmes de fonctionnement de l'unité administrative ; la rétention d'information ; la conservation de documents de valeur inégale ou non-conservation d'information à valeur probante ; la mauvaise conservation matérielle des documents ; la perte ou élimination de documents et de dossiers essentiels au fonctionnement de l'institution ; le non-respect de la confidentialité des informations ; le manque de fiabilité de l'information ; la mauvaise information qui engendre une mauvaise prise de décision ; le temps perdu à rechercher des documents et des dossiers mal classés ; le manque de place pour la documentation (Uniris 2016).

D'autres auteurs comme Smallwood ne présentent, ni ne catégorisent les risques informationnels, mais proposent de lister ceux qui sont propres à une entreprise et de relever leur impact (Smallwood 2014). La confédération suisse propose aussi cette démarche pour l'ensemble des risques (DEFR 2017). Desroches renonce aussi à une classification des risques informationnels. Elle a mené des entretiens dans les entreprises, relevé quelques risques, mais ne s'intéresse pas à leur catégorisation ou à leur traitement. Elle se concentre sur le rôle du gestionnaire de la sécurité (Desroches 2013). Lemieux (2004a) rappelle que le risque informationnel n'est souvent pas reconnu comme un type de risque à part entière, que les risques à l'intérieur de cette catégorie ne sont pas répertoriés et qu'ils se fondent dans d'autres catégories (juridique, financier, de réputation, etc.). Elle invite à prendre conscience de leur existence et à les faire gérer par des professionnels. Elle cite quelques exemples où la gestion de l'information est source de problèmes ou risques dans divers contextes. Comme

les auteurs précédents elle liste les événements qui nuisent aux records (tableau ci-dessous) (Lemieux 2004a).

Figure 4 : Risque informationnel, cause ou conséquence

Sector(s)	Primary Risk	Secondary Risk(s)	Cause of Risk	Consequence of Risk
Investment Banking	Legal[a] and regulatory risk	Financial[b] and reputational risks[c]	Failure to preserve e-mail in accordance with Securities and Exchange Commission rules	$1.65 (U.S.) million fine each against five investment banks

Trigger Event	Risk	Risk Mitigation Strategy	Owner of Risk Mitigation Strategy
Disaster – Natural or human caused (e.g., fire, flood, earthquake)	Loss or damage to records and information	Disaster preparedness and recovery program	Business continuity planning group and/or records management

(Lemieux 2004a, p.35-36, 45)

Au niveau du droit, les juristes et avocats sont essentiellement confrontés au « risque de voir une information appréhendée contre la volonté de son détenteur » (vol, effacement...) et « la diffusion de fausses informations, d'informations mensongères de manière volontaire ou non » (Du Manoir de Juaye 2014, p.37). Comme évoqué dans le chapitre précédent, on ne peut pas négliger ou exclure ce dernier type de risques à l'ère du numérique, même s'il sera peut-être moins représentatif dans notre étude qui se concentre sur les centres de documentation ou ressources informationnelles des organisations. Rouaud et Barriol (2012), dans une étude des risques et opportunités liés à l'e-réputation des entreprises, évoquent plusieurs procédés d'atteintes à l'e-réputation d'une entreprise. Ils parlent d'atteintes informationnelles comme la diffusion d'avis négatifs de consommateurs, le dénigrement, la rumeur et la diffusion de fausses informations.

Du côté de l'intelligence économique ou des sciences de la communication, nous retrouvons aussi les risques liés à l'information « message », la communication. Harbulot (2005), par exemple, cite des techniques d'attaque par l'information, comme occuper le terrain par la connaissance (mieux parler que l'autre, s'appuyer sur la société civile, etc.) ou déstabiliser par l'information (identifier les points faibles de l'adversaire, utiliser l'art de la polémique, utiliser l'opinion publique, etc.). « L'entreprise doit apprendre à détecter le risque informationnel et ne pas se laisser déstabiliser par l'information », dit-il. (Harbulot 2005)

Le guide du routard de l'intelligence économique, cité par Moinet (2014), liste aussi un certain nombre de risques informationnels comme par exemple : le questionnaire ouvertement intrusif d'un stagiaire ; l'appropriation de travaux de recherche par un jeune doctorant étranger ; la captation d'information stratégique via un simple appel téléphonique ; l'audit intrusif ; la mise en ligne d'informations confidentielles sur un blog ; la divulgation d'informations stratégiques lors de l'utilisation d'un traducteur en ligne *;* les résultats de la recherche d'une PME française brevetés à l'étranger par un post-doctorant ; la livraison d'informations à une puissance étrangère ; le transfert massif de données à l'étranger ; la désorganisation et la fragilisation par des méthodes de veille technologique déloyales ; l'imposition de clauses intrusives à un distributeur français ; la contrefaçon d'innovation par un partenaire commercial ; les atteintes à la réputation, comme par exemple une campagne calomnieuse à l'encontre du produit d'un concurrent, etc. (Moinet 2014).

Le listage des risques informationnels est critiqué par Moinet. Il estime qu'« établir un inventaire ou une liste de risques informationnels relève d'une vision statique, génère plus un sentiment de paralysie qu'elle n'offre au responsable l'agilité qu'il recherche » (Moinet 2014, p.44). Il rappelle que l'information circule, qu'elle peut s'enrichir en circulant, mais qu'elle est aussi périssable. Il faut « maîtriser l'information stratégique pour accroître sa position concurrentielle » (Moinet 2014, p.44). Agilité, rapidité, efficacité et coût sont les mots d'ordre dans l'économie de l'immatériel. Évaluer les mesures de protection présente peut-être davantage d'inconvénients que d'avantages (Moinet 2014). Sa théorie est intéressante dans son domaine où l'information est indissociable de la communication, mais peut-être moins dans la gestion ou la sécurité des actifs informationnels à long terme.

Au final, nous avons des menaces, événements déclencheurs qui impactent l'information, la documentation ou les actifs informationnels. Les types de risques informationnels sont ici essentiellement la perte, l'endommagement, la destruction, la modification ou le vol des informations. Et puis nous avons les risques informationnels déclencheurs ou sources de problèmes ou qui peuvent avoir des effets négatifs par ex. sur les finances ou la réputation d'une société. Les types de risques informationnels sont ici aussi bien la mauvaise gestion de l'information que les atteintes informationnelles telles la divulgation, la diffusion d'avis négatifs ou de fausses informations. Vermeys résume le tout ainsi : les risques associés à la notion de sécurité informationnelle se limitent à la divulgation, la destruction et la modification, intentionnelle ou non, des données. Il s'agit toujours de préserver l'intégrité, la confidentialité, mais aussi la disponibilité des données : on ne peut limiter les risques en empêchant l'accès à ces dernières (Vermeys 2009).

2.7 Evaluation des risques

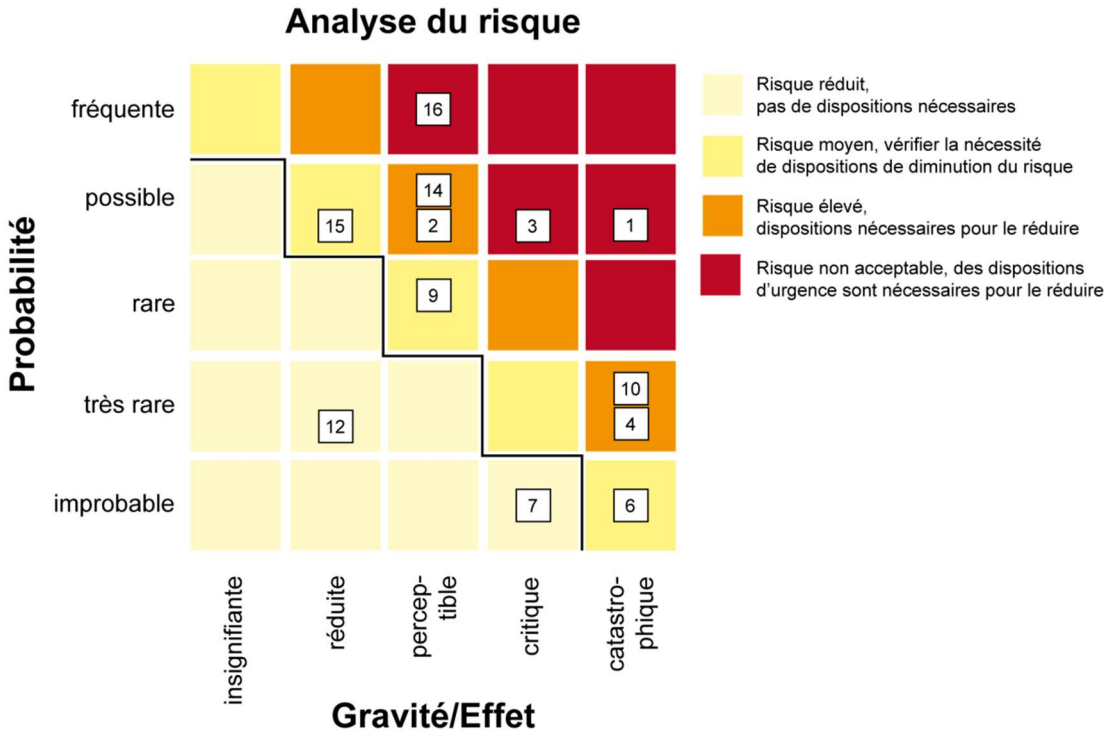
Après l'identification des risques, beaucoup d'auteurs proposent de décrire les risques ou les scénarios de risques qui intègrent des notions de temps, lieux ou processus (Clusif 2009). Ainsi, on s'assure que tous les acteurs le comprennent et parlent du même risque. On commence à rédiger une fiche pour chaque risque (cf. annexe 1). On la complète au fil du processus de la gestion des risques (modèle de l'AFF 2015 ; DEFR 2017 ; Léger 2013 ; Lemieux 2004,). Comme cette tâche de description est longue et coûteuse, on définit et évalue les risques les plus significatifs pour l'entreprise, ceux qu'il faut traiter de manière prioritaire. On parle de priorisation des risques. Le portail PME dit : « l'expérience montre que les entreprises se focalisent souvent sur 10 principaux risques environ » (DEFR 2017).

Les risques sont généralement hiérarchisés suivant leur gravité et leur probabilité d'occurrence. Les méthodes d'analyse de risque varient d'une entreprise à l'autre et d'un ouvrage à l'autre (Darsa 2013, DEFR 2017). La plupart combinent des analyses qualitatives (échelle d'attributs qualitatifs) et quantitatives (échelles avec valeurs numériques) (ISO/CEI 27005 :2011, Léger 2013, Lemieux 2004a). Lemieux cite aussi les principes à respecter pour la mesure du risque : « objectivity, consistency, relevance, transparency, firm-wide et completeness » (Lemieux 2004a, p.27-28).

Une démarche assez simple est proposée sur le portail PME de la Confédération suisse. On s'efforce, ici, de fournir des informations et des outils utiles aux PME. Le risque est évalué sur deux dimensions : la probabilité (aussi appelée fréquence) et les conséquences. La probabilité est la vraisemblance qu'un événement survienne sur une période définie et les conséquences décrivent l'effet que produit réellement l'événement (DEFR 2017). Les conséquences sont

souvent financières. Mais il peut aussi y avoir des dommages corporels, des atteintes à la réputation, des entraves aux processus opérationnels et des conséquences environnementales ou juridiques, etc. (AFF 2015). Desroches ou Lemieux proposent aussi d'effectuer le calcul du risque à partir de ces deux éléments (Desroches 2013, Lemieux 2004a). Les risques sont ensuite cartographiés, présentés graphiquement comme par ex. ci-dessous.

Figure 5 : Analyse du risque



(Risikomanagement, Schweiz. Vereinigung für Qualitäts- und Management-Systeme (SQS), Zollikofen; 2008, cité par DEFR 2017)

Une interprétation selon Hassid 2008 :

> *« [1] Les risques de fréquence et de gravité faibles : ce sont des risques mineurs qui se réalisent rarement, dont les impacts sont limités. L'entreprise peut vivre avec ses risques.*
>
> *[2] Les risques de fréquence faible et de gravité élevée : ce sont des risques qui se produisent rarement, mais dont les conséquences sont significatives. Il est difficile d'anticiper leur survenance. Le redémarrage de l'activité est coûteux ou n'est pas toujours possible. Ce sont les risques catastrophiques.*
>
> *[3] Les risques de fréquence élevée et de gravité faible : ces événements se produisent assez régulièrement, mais les conséquences sont limitées. Le risque peut être prévu ici. On parle de risque opérationnel.*
>
> *[4] Les risques de fréquence et de gravité élevées : ces risques sont évités. L'évaluation n'a que peu d'intérêt. Le plus souvent, le décideur abandonne le projet, à moins qu'il le considère comme une chance inestimable pour le développement de son entreprise.*
>
> *L'entreprise se focalise surtout sur les risques 2 et 3 »* (Hassid 2008, p.54-56)

Mayer et Humbert (2006) proposent une équation du risque qui est couramment utilisée, selon eux : RISQUE = MENACE x VULNÉRABILITÉ x IMPACT. Une menace correspond à un type

d'action bien identifié qui peut nuire. La notion de menace est aussi expliquée par le Clusif. Elle n'est pas strictement liée à la cause du risque, mais permet de définir, en fonction de listes de menaces types, des typologies de risques (Clusif 2009). Léger en dresse une liste dans le domaine de l'information (Léger 2013). La vulnérabilité correspond au niveau d'exposition face à la menace (Eduscol 2015, Léger 2013). Cette notion est généralement utilisée dès que l'on aborde la sécurité des systèmes d'information (Clusif 2009). C'est la caractéristique d'un asset (actif) constituant une faiblesse ou une faille au regard de la sécurité. Enfin l'impact représente la conséquence du risque sur l'organisme et ses objectifs. La menace et la vulnérabilité, représentant la cause du risque, peuvent être qualifiées en termes de potentialité. L'impact peut, quant à lui, être qualifié en termes de niveau de sévérité ou gravité (Mayer et Humbert 2006). Vermeys, qui propose aussi cette équation ajoute qu'il est impossible de contrôler le risque, mais qu'il est possible d'agir sur les vulnérabilités, ce qui affecte indirectement les menaces. Il cite quatre catégories de vulnérabilités : les vulnérabilités techniques, physiques, opérationnelles et celles liées à la gestion du personnel. Les menaces sont regroupées en 6 catégories : humaines, naturelles, techniques, physiques, environnementales ou sanitaires, opérationnelles. Pour leur faire face, il faut agir sur les vulnérabilités, adopter des contre-mesures techniques, physiques, opérationnelles et des contre-mesures liées à la gestion du personnel (Vermeys 2009).

L'identification des risques, leur classement et modélisation permet de mieux les comprendre et facilite leur analyse. L'évaluation et la mesure des risques, le listage des menaces et conséquences permettent d'appréhender les risques, de les prioriser et déterminer un seuil de tolérance au risque. Si les risques sont situés au-delà de ce seuil, ils ne doivent pas être tolérés (DEFR 2017, AFF 2015). L'évaluation et l'analyse des risques invitent à réfléchir aux risques, planifier des actions et à mieux agir s'ils surviennent. S'il reste une part de risque après l'application des techniques de gestion des risques, on l'appelle risque résiduel.

2.8 Traitement des risques informationnels

Le résultat ou la suite du processus cité dans le point précédent est le plan de mitigation des risques informationnels, ce plan doit contenir la liste des risques trouvés au processus de listage et d'évaluation, il doit contenir des échéanciers et assigner des rôles et responsabilités (Smallwood 2014). Par la suite il faudrait pouvoir évaluer objectivement le bon fonctionnement du plan par le développement de métriques (qui seront aussi utiles pour les audits) et le mettre en exécution en ayant recours à des outils spécifiques et en consultant régulièrement les équipes (Smallwood 2014).

Selon le risque plusieurs types de mitigation peuvent être instaurés, ces mesures de réduction peuvent être techniques, organisationnelles et juridiques selon Rouhier (2008).

« [Les étapes du management des risques] amènent le gestionnaire à hiérarchiser les risques et à déterminer quelles actions [de mitigation] doivent être privilégiées. » (Desroches 2013, p.12) Le choix d'une de ces actions sera lié, entre autres, à la connaissance qu'a le gestionnaire des risques passés, actuels et du contexte dans lequel évolue l'entreprise (Desroches 2013).

Une fois les risques identifiés et classés par priorité, il faut établir les mesures de mobilisation en cas de survenue de ce risque, qui sont généralement : ignorer le risque consciemment, l'éviter en renonçant à poursuivre une activité, l'accepter, le mitiger par des mécanismes de protection, ou le transférer via une assurance ou l'externaliser (Léger 2013, p.29). Pierandrei cite ces mêmes mesures : évitement, prévention, acceptation et transfert. Il rappelle que « le coût de la gestion du risque ne doit pas excéder l'impact de la perte potentielle qu'elle est censée couvrir ». Dans un milieu compétitif où on maximise le profit, ce sont surtout des stratégies de prévention et d'auto-assurance que le risk manager élabore (Pierandrei 2015, p.55-56). Lemieux dit que la gestion des documents est souvent externalisée : « it's increasingly common for financial institutions to outsource records storage, tape storage and the performance of traditional records management functions » (Lemieux 2011, p.133). L'externalisation présente de nombreux avantages, mais n'est pas sans risque : Lemieux parle de « data loss or leakage, compliance failures, business continuity concerns and loss of organisational knowledge ». L'externalisation est complexe et doit être planifiée. Toute la stratégie et les processus de l'outsourcing sont décrits par Lemieux (2011).

Si la décision pointe vers l'acceptation des risques, il faut établir des critères d'acceptation élaborés et spécifiés qui dépendent directement des politiques de l'organisation (ISO/CEI 27005:2001, p.13), ils peuvent être exprimés comme un rapport entre le profit estimé et le risque estimé, ils peuvent varier selon la durée d'existence du risque et différents critères d'acceptation peuvent s'appliquer (ISO/CEI 27005:2001).

Léger (2013) propose le modèle des 3 P (prévention, protection, punition) pour la mise en œuvre de la sécurité de l'information sur le terrain : la prévention par des mesures telles que politique de sécurité, processus formel d'analyse des risques, audits annuels et formation et sensibilisation des utilisateurs), la protection par les actions de mitigation du risque (allocation des responsabilités à des individus, mise en œuvre des processus de gestion des incidents, de recouvrement en cas de sinistres et de continuité d'affaires) et la punition en cas de non-respect des deux premiers axes. Il mentionne aussi les mesures de détection pour alerter l'organisation en cas de problème survenu et mesures de réponse face aux conséquences (Léger 2013, p.18).

Lemieux mentionne aussi l'évitement, le transfert, l'acceptation et ajoute deux mesures : réduction de sa probabilité et réduction de son impact (Lemieux 2004a, p.20). Elle mentionne que dans la plupart des grandes organisations, la responsabilité pour la mitigation d'un certain type de risque sera assignée à des domaines particuliers de l'entreprise et propose un tableau avec des exemples de quelques-unes des stratégies de mitigation les plus courantes en risques informationnels et les propriétaires du risque (Lemieux, 2004, p.45) :

Figure 6 : Exemples de traitement des risques

Trigger Event	Risk	Risk Mitigation Strategy	Owner of Risk Mitigation Strategy
Disaster – Natural or human caused (e.g., fire, flood, earthquake)	Loss or damage to records and information	Disaster preparedness and recovery program	Business continuity planning group and/or records management
Major system outages or disruptions caused by system or human errors	Loss or damage to records and information	System backup and recovery strategy	Business continuity planning and/or IT group
Computer fraud	Loss of funds	IT security strategy	IT security group
Theft of electronic information and electronic information assets	Loss of critical business information potentially leading to possible loss of funds or damage to reputation	IT security strategy	IT security group
Theft of computer system resources (e.g., use of organization's computer systems for other than official purposes)	Loss of funds or damage to reputation	IT security strategy	IT security group
Malicious attacks and harmful code (e.g., virus attacks, hackers, etc.)	Loss of critical business information and/or funds	IT security	IT security group
Unauthorized disclosure of electronic information	Loss of confidentiality of business information, leading to possible loss of funds and/or damage to reputation	IT security	IT security group
Errors and omissions in documentation	Critical business information missing, resulting in an inability to enforce a contract and/or third-party liability, and possibly leading to loss of funds and/or damage to reputation	Documentation procedures	Legal and/or line of business
Inadequate retention periods for records and information	Records and information unavailable, resulting in noncompliance with laws and regulations and/or inability to enforce contracts or support litigation and possibly leading to loss of funds and/or damage to reputation	Retention scheduling	Legal and/or records management group

(Lemieux 2004b, p.58)

Il faut prendre en compte que cette étape n'est pas à part, « le traitement des risques implique un processus cyclique d'appréciation d'un traitement des risques, (...) de reconnaître si les niveaux de risques résiduels sont acceptables, [et si ce n'est pas le cas, de commencer] un nouveau traitement des risques et appréciation de l'efficacité du traitement considéré ». (ISO/CEI 27005:2001, p.10). Les risques résiduels doivent être explicitement acceptés par les dirigeants (ISO/CEI 27005:2001, p.10).

Plusieurs types de mesures sont possibles, il y en a autant qu'il y a de causes ou même davantage. « Il convient de choisir des mesures de sécurité adaptées et justifiées afin de répondre aux exigences identifiées par l'appréciation et le traitement des risques » (ISO/CEI 27005:2001, p.27). Le choix sera fait en prenant en considération les **exigences légales**, réglementaires et contractuelles, en raison des coûts d'acquisition, du délai de sa mise en œuvre, de la facilité d'utilisation, des aspects techniques, environnementaux et culturels (ISO/CEI 27005:2001), et aussi en procédant à une **évaluation des contraintes** liées à ces mesures : techniques, de coût opérationnel, des problèmes de compatibilité, niveau de

difficulté pouvant mener à des erreurs humaines ou altération des performances (ISO/CEI 27005:2001).

Quelques exemples de mesures de sécurité :

- Politique de protection de l'information
- La définition d'un Disaster recovery plan (DRP) ou plan de secours pour permettre à l'entreprise de démarrer plus rapidement en cas de crise avec le moins de pertes. (Lacroix 2007)
- Conformité des systèmes d'information, audits (Lacroix 2007)
- Sécurité des systèmes d'information, outils techniques (pare-feu, identification, antivirus, contrôle d'accès) (Lacroix 2007, Caprioli 2007)
- Plan de continuité d'activité (Lacroix 2007, p. 44) - possibilité de continuer à travailler depuis un autre endroit en cas d'un problème géographiquement localisé.
- Education, sensibilisation, communication (Smallwood 2014, Lacroix 2007)
- Gestion du risque par le transfert : assurances, etc. (Lacroix 2007, Caprioli 2007)

A ce propos et concernant spécifiquement le risque informationnel : « Le transfert de risque est rarement une solution acceptable en matière de système d'information » (Lacroix 2007, p.41) ce qui amène plutôt à un choix « de traitements par réduction des risques (plans d'actions) » (Lacroix 2007, p.41).

Une mesure de sécurité peut être reconnue comme inefficace, dans ce cas il convient de la contrôler pour déterminer si elle doit être retirée, remplacée ou laissée en place par des raisons de coûts par exemple (ISO/CEI 27005:2001).

Pour plus de types de risques informationnels et respectives mesures à prendre consultez l'ISO/CEI 27005. Les annexes C et D présentent une longue liste avec des menaces types et vulnérabilités suivies des méthodes d'appréciation.

2.9 Deux approches

Lemieux (2004B) propose deux types d'approches pour la gestion des risques informationnels :

Basée sur les événements (« event-based ») - cette approche part de du problème existant, des défaillances. On identifie les facteurs qui pourraient être source de risque, on les liste pour faire ensuite leur traitement. C'est une approche en quelque sorte *bottom up* et plutôt défensive.

Basée sur les exigences informationnelles (« Records and information requirements-based ») - Cette approche, plus dirigée vers les objectifs à atteindre, décide des qualités que l'information circulant dans l'organisation doivent avoir. A partir de ce constat on identifie ce qui pourrait poser problème dans l'atteinte de ces objectifs. C'est *top down*. Plus orientée stratégie et plus efficace pour identifier les problèmes et opportunités de façon systémique. Favorise la coopération transversale.

Toutes les deux auraient leurs avantages et inconvénients, leur utilisation dépendrait des besoins et du contexte de l'entreprise, du temps ou budget à disposition. La deuxième serait la plus coûteuse et plus complexe à instaurer, mais avec plus d'avantages stratégiques.

2.10 Normes liées à la gestion du risque informationnel

Dans cette partie nous abordons les réglementations touchant les risques informationnels du point de vue des normes et des lois.

2.10.1 Normes de conformité

Il y a deux types de normes : « de jure et de facto » (Smallwood 2014, p.76) : les normes « de jure » sont celles publiées par des organismes de normalisation reconnus, tels que l'Organisation internationale pour Standardisation (ISO), American National Standards Institute (ANSI), British Standards Institute (BSI), etc. Les normes « de facto » ne sont pas des normes formelles mais sont considérées par beaucoup comme si elles l'étaient. Elles peuvent se manifester par une utilisation populaire (par exemple Windows dans la décennie 2001-2010) ou peuvent être publiées par d'autres organismes, tels que la National Archives and Records Administration aux États-Unis (NARA) ou par les Organismes de normalisation sans avoir le statut formel d'un « standard » (tel certains rapports techniques publiés par l'ISO) (Smallwood 2014, p.77).

La normalisation de l'archivage (qui représente un aspect de la gestion de l'information), par exemple, est prise en charge par différents organismes comme l'Association française de normalisation (Afnor) en France, l'Organisation internationale de normalisation (ISO) ou le Conseil international des archives (CIA) au niveau international.

Les normes présentent certains avantages tels qu'une assurance de qualité, elles peuvent servir de guides à des projets, présentent une uniformité de nomenclatures et pratiques et proviennent d'un consensus international (Smallwood 2014, p.77). Les points négatifs sont la possibilité de réduire la flexibilité et par conséquent l'innovation ; la norme peut se baser sur des règles et terminologies moins adaptées au contexte que les normes locales, et sont surtout basées sur la théorie (Smallwood 2014, p.77).

Les normes élaborées par l'ISO, principale organisation internationale de normalisation, sont créées par consensus et ont des limites, une fois qu'elles sont élaborées à partir d'un « dénominateur commun à l'ensemble des participants (...) [et qu'il y a possibilité] que des groupes d'intérêts particuliers (...) ou financiers viennent influencer le processus, en particulier quand il y a des enjeux de vente de produits ou de services à la clef, comme c'est le cas avec la norme ISO 27005 ». (Léger 2013, p.130). Il précise que « Dans le cas des normes dans le secteur des TIC, l'ISO travaille en étroite collaboration avec la CEI (Commission électrotechnique internationale) chargée des domaines de l'électricité, de l'électronique et des techniques connexes » (Léger 2013, p.130).

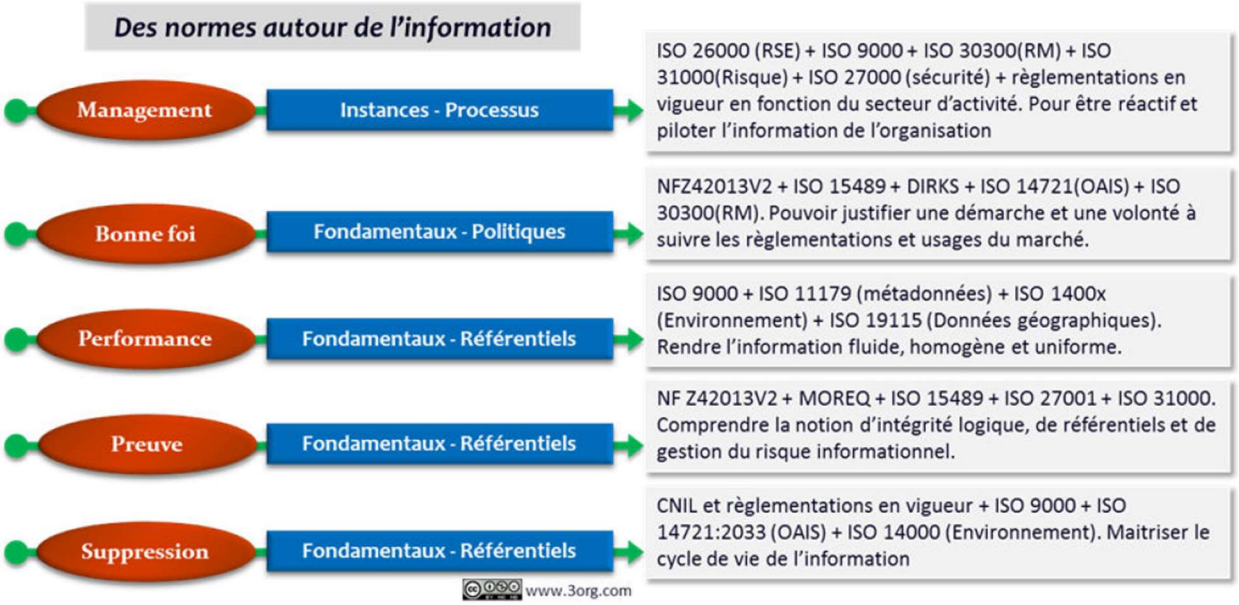
Plusieurs normes touchent la gestion et la sécurité de l'information. Une liste regroupant les principales est fournie en annexe 2. Certains auteurs les classent comme suit :

Classification de normes par Smallwood 2014 :

- Gestion des risques : ISO 31000

- Gouvernance et sécurité de l'Information : ISO/CEI 27001 et ISO/CEI 27002, ISO/CEI 38500
- Records and E-Records Management : ISO 15489, ISO 30300 series.

Figure 7 : Classification des normes autour de l'information



(Observatoire de la gouvernance de l'information et 3ORG conseil 2012, p.29)

2.10.2 Normes relatives aux domaines spécifiques

Certains domaines ont leurs propres normes. Aborder la totalité des normes de chacun étant impossible dans le cadre de ce travail, nous citerons comme exemple le domaine financier.

La gestion des risques en milieu bancaire est bien développée et cadrée. On parle d'Enterprise Risk Management (ERM) depuis les années 90. Les banques sont, en principe, soumises au contrôle ordinaire et doivent mettre en place un système de contrôle interne et gestion du risque. Elles utilisent généralement le référentiel COSO dont un des composants est l'évaluation des risques. Ce référentiel est revu périodiquement. COSO 2013 tient compte, par exemple, de l'émergence de nouveaux risques et de la vulnérabilité des systèmes d'information (atteinte à l'e-réputation, cloud computing et perte de confidentialité des données, cybercriminalité…) (Pierandrei 2015).

Le risque informationnel n'est pas directement mentionné, mais en regardant en détail, un des objectifs du COSO2 est « la fiabilité des informations financières » et une des cinq composantes du contrôle interne pour ce référentiel est « l'information et la communication » à optimiser via une analyse constante des informations du passé, du présent et des informations probables concernant les performances de l'organisation pour détecter « des potentiels événements futurs qui affectent le profil de risques actuel de l'organisation », une composante importante est « la nécessité de s'assurer que la granularité des informations

(niveau de détail et périodicité), est suffisante pour identifier, analyser, et répondre aux risques et ainsi rester dans les limites de son appétence au risque[4] ».

2.11 Lois

La mise en place d'un projet de gestion de risques est constituée de plusieurs étapes comme nous l'avons vu. Cependant, il faut être attentif à une étape qui précède à toutes les autres : l'enquête sur les normes juridiques réglementaires qui s'appliquent à l'entreprise :

> *« There are federal, provincial, state, and even municipal laws and regulations that may apply to the retention of information (data, documents, and records). Organizations operating in multiple jurisdictions must maintain compliance with laws and regulations that may cross national, state, or provincial boundaries. Legally required privacy requirements and retention periods must be researched for each jurisdiction (e.g. county, state, country) in which the business operates, so that it complies with all applicable laws ».* (Smallwood 2014, p. 43)

Il est essentiel de situer l'entreprise dans son environnement légal :

> *« Legal requirements trump all others. The retention period for a particular type of document or PII data or records series must meet minimum retention, privacy, and security requirements as mandated by law. Business needs and other considerations are secondary. So, legal research is required before determining and implementing retention periods, privacy policies, and security measures* (Smallwood 2014, p.43) *».*

Avoir recours à la législation sert à se protéger (puisque enfreindre une loi est un risque qu'il faut maîtriser) mais pas uniquement : on peut aussi faire usage des outils juridiques pour protéger le patrimoine informationnel.

« Il s'agit de la maîtrise, la valorisation et la protection du patrimoine informationnel appartenant à une entité publique ou privée, par la mise en place de procédés légaux, réglementaires, contractuels ou organisationnels » (Caprioli 2007, p.33) comme par exemple, établir une politique de sécurité des systèmes d'information, une charte d'utilisation des communications électroniques, contrats de travail et règlements intérieurs, contrats avec tiers (utilisation encadrée et contrôlée des stagiaires, prestataires externes, sous-traitants qui utilisent le système) et avoir un guide juridique du DSI (Directeur des systèmes d'information) ou RSSI (Responsable Sécurité des Systèmes de l'Information) (Caprioli 2007).

L'information est aussi protégée par de nombreuses lois, nous citons comme exemple cette liste tirée de Caprioli 2007 :

- Le droit d'auteur
- Les droits sur les bases de données (dans le Code de la Propriété Intellectuelle)
- Le droit des brevets d'invention - titre délivré par l'INPI ou par l'Office européen des brevets (OEB) (Code de la Propriété Intellectuelle)
- Le droit des marques - (Code de la Propriété Intellectuelle) ; marque communautaire (règlement CE, Dépôt auprès de l'Organisation de l'harmonisation du marché intérieur OHMI. Dépôt au niveau international auprès de l'OMPI)

[4] COSO. *Wikipédia : l'encyclopédie libre* [en ligne]. Dernière modification de la page le 19 avril 2017 à 11 :17. [Consulté le 09 janvier 2018].

- Le droit des dessins et modèles - dépôt auprès de l'INPI ou OHMI pour le modèle communautaire.
- Le savoir-faire et secret de fabrique (Code de la Propriété Intellectuelle et Code du travail)
- Autres signes distinctifs : nom commercial, enseigne, dénomination sociale et nom de domaine
- Loi Informatique, Fichiers et Libertés
- Le droit de la responsabilité civile découlant du fait d'un salarié
- Code pénal - atteintes aux systèmes d'information

Il nous semble important de signaler que la liste ci-dessus mentionne plutôt les lois dans un contexte français, nous croyons qu'elles pourraient trouver leur équivalent dans d'autres juridictions.

En Suisse, nous trouvons des lois fédérales, cantonales et des lois sur la protection de données. En voici quelques-unes[5] :

- Ordonnance concernant la protection des informations de la Confédération 2007 (2016)
- LPD, Loi Fédérale sur la protection des données
- LIPAD, Loi sur l'information du public, l'accès aux documents et la protection des données personnelles (Canton de Genève)
- LAr, Loi fédérale sur l'archivage
- LArch, Loi sur les archives publiques (Canton de Genève)
- Ltrans, Loi fédérale sur le principe de la transparence dans l'administration
- Lois métier : selon nos recherches et en faisant des comparaisons, certaines lois métiers de certains cantons seraient plus sensibles à la question de la protection de l'information que d'autres.

Le sujet est vaste et complexe. Il serait intéressant de le creuser par des analyses comparatives entre cantons ou pays.

2.12 Logiciels, outils pour l'analyse des risques informationnels

> *« Pour l'identification, l'analyse et le traitement des risques liés aux systèmes d'information (...) il existe de nombreuses méthodologies à la disposition de la DSI. Ces méthodologies (Méhari, Ebios...) proposent un déroulé pas à pas du processus de gestion des risques liés aux systèmes d'information. Néanmoins, ces méthodes d'analyse apparaissent aux yeux de certains DSI, trop lourdes et difficilement adaptables aux contraintes et spécificités de leur entreprise, (...) leur application dans un environnement nouveau implique des ajustements difficiles à mettre en œuvre. Pour cette raison, de nombreuses entreprises n'appliquent pas stricto sensu ces méthodes. Néanmoins, elles peuvent s'en inspirer pour mettre en place leurs propres procédures d'analyse et de traitement des risques »* (Lacroix 2007, p.43).

[5] Pour une liste avec plus de détails consulter : http://www.archives.ch/utile/legislation.php et http://vsa-aas.ch/wp-content/uploads/2015/07/BAR_Bases_legales_de_gestion_des_documents_et_d_archivage.pdf

En ce qui concerne les méthodologies utilisées par les départements de sécurité de l'information, les DSI « s'appuient en général sur un référentiel à trois niveaux : la politique globale de sécurité et de gestion des risques, menée au niveau groupe; les standards , normes ISO, le plan de continuité informatique (PCI), les réglementations, etc. et les méthodologies : le directeur des risques peut (...) appliquer certaines méthodologies du marché pour appréhender le risque lié aux systèmes d'informations (MEHARI, EBIOS, ITIL etc.) » (Lacroix 2007, p.35)

2.12.1 Politiques de sécurité

« Les politiques sont l'ensemble des règles qui sont en général expliquées à travers un document. Si ces politiques sont formalisées et font partie d'une liste ou d'un ensemble spécifique structuré, alors cela devient un référentiel de règles. La politique explique les règles, le référentiel les rend exploitable. » (Observatoire de la gouvernance de l'information et 3ORG conseil 2012, p.13) La politique propose l'utilisation des méthodologies et d'outils et sert comme point de référence pour ce qui est autorisé ou interdit à l'ensemble de l'entreprise pour que tous puissent participer de façon globale à la gestion des risques.

La politique de sécurité inclut entre autres (Leger 2013, p.16) :

- la politique de gestion des risques
- la catégorisation et l'étiquetage de l'information
- la sécurité du personnel et du matériel
- les exigences juridiques et contractuelles
- l'élaboration et le fonctionnement des systèmes
- la production des rapports sur les incidents
- l'application de mesures en cas de violation
- la sensibilisation à la sécurité et la formation

> *« La politique la plus active, dans le sens « validée » et « diffusée », est celle concernant les données personnelles (cf. CNIL). A l'opposé, celle décrivant la protection du patrimoine informationnel (connaissance, brevet, secret) se retrouve en avant-dernière position. La donnée à caractère personnel est une notion qui nous touche fortement, et spontanément : on parle de droit à l'oubli, de bonne (ou mauvaise) réputation (...). La protection du patrimoine informationnel est une notion qui concerne au contraire de nombreuses données diffuses, et son application dépend des appréciations de risque que peuvent développer les individus. »* (Observatoire de la gouvernance de l'information et 3ORG conseil 2012, p.45)

2.12.2 Méthodes et outils

Dans l'annexe 3, nous présentons une liste de méthodes et outils, elle est large et non exhaustive : chaque méthodologie a ses limites et elles ne sont pas prêtes à l'emploi. Chaque organisme se sert de ces outils en faisant des adaptations, en plus il y a certaines entreprises qui préfèrent créer une méthodologie « maison ».

Dans un article dans lequel il présente une grille d'analyse des méthodes d'analyse de risque, Léger estime que « CRAMM, EBIOS et Octave semblent supérieures. Méhari nécessite un encadrement. Les autres méthodes sont immatures ou invérifiables » (Léger 2015c).

2.13 Rôles et responsabilités en gestion du risque informationnel

Les SI, systèmes d'information, sont à la fois des sources de risque et un moyen de les gérer (Eduscol 2015, p.3). Le rôle joué par la direction des systèmes d'information est donc opérationnel et stratégique. Mais quelle est sa place dans l'organigramme de l'entreprise ?

Pour aborder cette question, nous commençons par situer la place du Risk manager, qui reflète le niveau de maturité en gestion des risques de l'entreprise (Lacroix 2007). Cette place dépend de la stratégie de l'entreprise.

Lacroix nous présente 4 modèles d'organigrammes possibles en gestion de risques (Lacroix 2007, p.20) :

- Organisation « globale » - Liée à l'adoption d'une politique globale et intégrée de gestion des risques d'entreprise. Le risk manager est le plus souvent rattaché au comité exécutif qui définit avec son aide, les éléments de la politique générale de gestion des risques.
- Organisation « centrale réduite » - Généralement adoptée par les entreprises fortement centralisées ou mono-sites en gestion des risques. Assisté d'une petite équipe, le risk manager du Groupe définit la politique générale de gestion des risques assisté d'une petite équipe et est en dialogue permanent avec les directeurs métiers et les opérationnels avec lesquels il établit la cartographie des risques et les plans d'action nécessaire à leur traitement. Normalement, il n'y a pas de correspondants risques ou équivalents dans les filiales.
- Organisation en « électron libre » - Il n'y a pas de risk manager, mais il y a une démarche de gestion des risques initiée par une direction métier ou fonctionnelle. Liée à l'absence d'une politique de gestion de risques globale, la démarche peut être inefficace.
- Absence d'organisation - Quand il n'y a pas de risk manager, ni de démarche structurée de gestion des risques, les métiers gèrent leurs risques localement et indépendamment et non au niveau du Groupe.

2.13.1 Relation risk manager et DSI

La DSI participe à la gestion des risques propres ou liées aux SI. « La DSI peut contribuer fortement à la démarche de risk management. Cette contribution s'exerce alors généralement sous la forme d'une influence directe lors de la mise en œuvre d'une politique globale et intégrée de gestion des risques dans l'entreprise ou indirectement par la mise en place d'outils, de méthodes ou de formations en support aux activités du risk manager. » (Lacroix 2007, p.37)

Les directions isque et SI peuvent coopérer, elles ont une culture de la sécurité commune et la DSI a une forte culture en gestion des risques (Lacroix 2007). Ces deux directions sont parfois rattachées au même directeur (Lacroix 2007). » La sécurité des SI se situe donc au niveau opérationnel et tactique, en réponse aux risques identifiés au niveau stratégique ». (Eduscol 2015, p.4)

Quand il y a un Responsable de la sécurité du système d'information, RSSI, dans l'entreprise, il doit concilier ses aptitudes techniques et managériales, il connaît les métiers de son entreprise et de l'organisation des SI, et est normalement amené à assurer des fonctions transverses, ce qui le fait toucher au domaine de la gestion des risques. (Eduscol 2015, p.4) Son rôle tend à évoluer, ses responsabilités touchent plusieurs domaines pour satisfaire aux

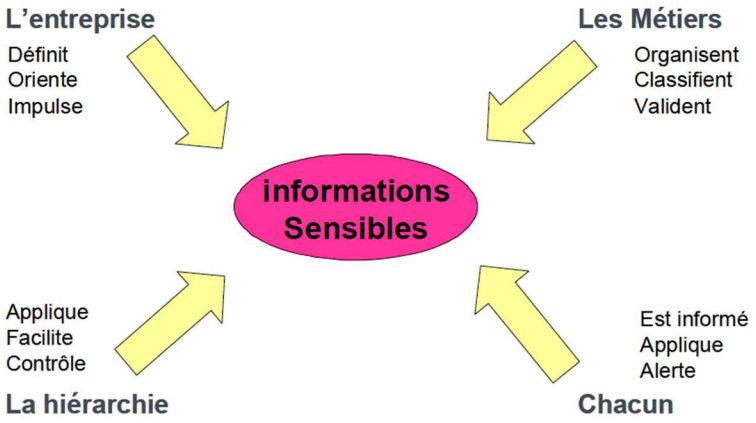
exigences de l'environnement, « le rôle du gestionnaire de la sécurité ne se limite plus à la protection physique des biens et des personnes : il doit maintenant veiller à protéger tant le patrimoine matériel qu'immatériel de l'organisation en s'assurant d'avoir les compétences et connaissances adéquates pour accomplir une telle tâche ou en s'alliant à des experts capables de le faire » (Desroches 2013, p.53)

Si les fonctions « gestionnaire de risque » et « RSSI » coexistent dans l'entreprise, leur coopération est nécessaire (Eduscol 2015, p.4).

Desroches suggère que trois aspects peuvent influencer significativement le processus décisionnel de gestion des risques informationnels : l'aspect contextuel, l'aspect relationnel (rapports entre départements, interaction entre employés, etc. ou en externe) et le profil du gestionnaire de la sécurité (Desroches 2013, p.96) qui peut être nommé de différentes façons : directeur des systèmes d'information, directeur de la sûreté, directeur de la sécurité globale, responsable des technologies de l'information, etc.

Le rôle du responsable est fondamental dans le processus de gestion de sécurité de l'information, il doit communiquer à plusieurs niveaux, à différentes parties prenantes qui intègrent le processus. Rouhier (2008) mentionne quatre acteurs principaux qui interviennent dans la protection de l'information : l'entreprise, la hiérarchie, les métiers et chacun individuellement.

Figure 8 : Les 4 acteurs dans la protection de l'information



(Renault/CIGREF, cité par Rouhier, 2008, p.13)

« Les fonctions RH, juridique, audit, services généraux, sont des co-acteurs importants qu'il faut impliquer complètement dans la démarche » (Rouhier 2008, p.14). L'utilisateur a également un rôle important, « il est le complément indispensable qu'il faut associer aux outils techniques/technologiques de valorisation et de sécurisation de l'information » (Observatoire de la gouvernance de l'information et 3ORG conseil 2012, p.23), il est donc important de l'écouter pour améliorer la productivité de l'entreprise.

Lemieux (2004b) dit que, dans la plupart des organisations, les responsables hiérarchiques traitent les risques liés aux documents et à l'information de manière ad hoc par le biais d'autres processus opérationnels comme l'informatique, la gestion de documents, l'audit, avec une approche orientée vers la prévention des pertes. Cependant, le nombre d'organisations qui prennent conscience de la nécessité de la gestion des risques liés à l'information au niveau du conseil d'administration et de la direction seraient en train d'augmenter, probablement à

cause des nouvelles lois et réglementations et pour éviter des pertes. Elle ajoute que, dans ces organisations, les RI sont généralement traités par le département concerné (par exemple, les catastrophes seraient traitées par un département, les menaces à la sécurité de l'information par un autre) et de façon ponctuelle.

Lemieux (2004b) signale aussi que la gestion des RI devrait être pleinement assimilée au programme de gestion des risques à l'échelle de l'entreprise et ce par le biais de son intégration au développement de la stratégie ; par la sensibilisation aux RI de façon à les insérer dans la culture organisationnelle par la mise en évidence de ces risques dans toutes les initiatives de formation, en définissant clairement les rôles et responsabilités en RI à tous les niveaux de l'organisation et en les reconnaissant comme composantes de tous les processus opérationnels et départements. Elle ajoute que le rôle des départements traditionnellement impliqués dans la gestion d'information (tels que records management ou IT) devrait être redéfini pour s'intégrer de façon adéquate au programme de gestion des RI à l'échelle de l'entreprise.

3. Méthodologie

3.1 Introduction

Nous avons procédé à une recension d'écrits théoriques comparés à la réalité sur le terrain en ce qui concerne la gestion des risques informationnels.

3.2 Revue de la littérature

Pour pouvoir cerner le sujet et travailler sur des bases scientifiques, nous avons d'abord fait une revue de la littérature. Les données pertinentes (sources) ont été choisies en fonction de l'objectif de la recherche : seul des documents provenant du milieu professionnel ou scientifique et qui avaient un rapport direct avec le sujet de recherche ont été analysés. Ensuite, ils ont été classés en trois groupes selon qu'ils provenaient de la recherche scientifique, de la littérature professionnelle (normes et standards, associations, consultants) ou qu'ils étaient rédigés dans le cadre d'une réglementation (lois, directives, réglementations). Pour limiter la taille du matériel à analyser, nous avons pris en compte les documents publiés en anglais et en français ces 15 dernières années (à l'exception de textes considérés comme de « référence »).

Les données trouvées au cours de nos lectures ont été étudiées au moyen de l'analyse de contenu qualitative. Cette approche méthodologique nous semblait la plus appropriée pour permettre « de fournir un résumé compréhensif d'un événement ou d'une situation » (Fortin et Gagnon 2016, p.191).

Le travail est de type exploratoire, des catégories ont été créés en fonction des objectifs traités pour pouvoir y classer les données et procéder à l'analyse. « En l'absence d'hypothèse de départ, le choix des catégories est difficile et devra naître du contenu. Il faut relire plusieurs fois le texte à analyser, pour dégager ce qui est essentiel par rapport à l'objectif de la recherche. » (Grawitz 2001) Ce qui a eu pour résultat la création de 8 catégories qui correspondent aux objectifs et aux questions de recherche. Un tableau a été créé avec le croisement de ces catégories et les trois groupes de sources consultées. Cette grille de lecture a été notre principal outil dans cette étape (annexe 4).

3.3 Entretiens semi-structurés

Pour avoir l'avis des spécialistes et vérifier si l'action sur le terrain corrobore aux écrits scientifiques, nous avons procédé à des entretiens semi-structurés.

3.3.1 Procédure d'échantillonnage

La présente recherche est de type qualitatif, les entretiens avaient pour objectif de nous permettre de comprendre la perception des professionnels sur le sujet étudié. Les personnes qui gèrent l'information au sein des diverses organisations ont constitué notre population cible. L'échantillon, non-probabiliste, a été choisi par convenance ou par choix raisonné.

Partant du principe que la gestion des risques pouvait changer selon le domaine de travail de l'entreprise, nous avons préféré choisir des organismes de 5 différents secteurs pour vérifier si les risques informationnels étaient gérés de façon spécifique au secteur concerné. Notre choix s'est porté sur les finances, la sécurité, la santé, la recherche et une organisation internationale (par son caractère multijuridiction). « (…) les archivistes doivent (…) prendre en

considération les lois et les règlements qui concernent le domaine d'activité dans le milieu au sein duquel ils évoluent. Pensons à la santé, à l'ingénierie ou aux municipalités, entre autres » (Leroux et al., 2010, p.38)

Les organismes interviewés ont été choisis en fonction de leur secteur de travail, leur emplacement (Suisse Romande) et de leur disponibilité pour participer à l'étude.

Nous avions prévu d'interviewer les responsables des ressources informationnelles, mais nous avons été redirigées vers les SI et les gestionnaires de risques à trois reprises. Nous avons finalement interviewé :

- Finances : Banque (B), records manager, responsable SI et le responsable de la gestion des risques
- Sécurité : Département de sécurité cantonal (DS), responsable d'archives
- Santé : Hôpital cantonal (HOP), responsable d'archives
- Recherche : Institution de recherche et enseignement (IRE), responsable SI
- Multijuridiction : Organisation Internationale (OI), responsable en gestion des risques

Les répondants avaient le choix de rester anonymes. Quatre sur cinq l'ont souhaité.

3.3.2 Collecte des données

La collecte des données a été faite sous forme d'entrevues semi-dirigées. Les questions ont été préparées suivant les huit catégories créées pour la grille de lecture (annexe 4) et selon la recension des écrits. Notre demande d'entretien (annexe 5) et le formulaire de consentement (annexe 6) sont en annexe de même que le questionnaire final (annexe 7). Les entretiens ont été enregistrés et transcrits.

3.3.3 Méthode d'analyse des données

Nous avons fait un tableau avec l'analyse des données issues de la transcription, puis une synthèse de ce qui est ressorti.

3.4 Validité et fiabilité de la recherche

3.4.1 Limites de l'échantillonnage

Notre échantillon est limité et, de ce fait, ne peut être représentatif de la totalité des entreprises en Suisse Romande.

3.4.2 Secret professionnel et confidentialité

Nous n'avons pas pu accéder à l'intégralité des informations utiles concernant la gestion des risques à cause des soucis de confidentialité. En fait, c'est aussi un sujet stratégique et les entreprises ne souhaitent pas rendre leurs faiblesses publiques.

3.4.3 Biais de désirabilité

Le biais de désirabilité « apparaît lorsque l'on collecte des données de manière auto-révélée. En effet, les individus ont tendance à se montrer aux chercheurs sous un jour plus favorable que ce à quoi l'on peut s'attendre. Ce biais est d'autant plus prononcé lorsque l'étude aborde des sujets qui pourraient embarrasser les répondants. » (Asseman et Dupont 2011, p.15).

Même si nous avons garanti la confidentialité aux répondants qui l'ont souhaité, l'interview n'a pas été faite de façon anonyme et a été enregistrée par un enregistreur vocal. On ne peut pas exclure, ici, l'influence de l'appréhension des répondants concernant le contenu de leurs réponses et l'accès à ces dernières d'autant plus que le sujet traité est sensible.

3.5 Conclusion

Même si la taille de l'échantillon n'est pas représentative, les données récoltées sont intéressantes et donnent des indications et des pistes pour d'autres travaux sur le même sujet. Le mieux serait d'interviewer davantage d'organisations (encore faut-il que des professionnels soient prêts à donner leur temps pour répondre aux questions) et le questionnaire pourrait être complètement anonymisé. L'idéal serait aussi que plusieurs personnes-clé dans la gestion de l'information de l'entreprise soient interviewées pour une meilleure vision d'ensemble.

4. Résultats

4.1 Introduction

Dans ce chapitre, nous faisons une synthèse des réponses que nous avons reçues lors de nos cinq entretiens. Nos apports et conclusions personnelles seront présentées dans le chapitre suivant.

Comme mentionné dans la partie méthodologie, nous avons interviewé une banque (B), une organisation internationale (OI), un département de sécurité d'un canton romand (DS), un hôpital cantonal (HOP) et un institut de recherche et d'enseignement (IRE).

A la banque, nous avons été reçues par le records manager, le responsable SI et le responsable de la gestion des risques ; à l'OI par un gestionnaire des risques ; dans le domaine de la recherche par le responsable SI qui est aussi gestionnaire des risques techniques ; à la sécurité et à l'hôpital par l'archiviste principal. L'interview idéale est celle où nous avions les différents corps de métier en présence. Dans le domaine de la recherche, nous aurions dû être orientées vers le gestionnaire des risques des ressources informationnelles comme le signalait le répondant, puisque nous avions plutôt affaire au domaine informatique et non informationnel. Le fait d'être dirigées d'un secteur à l'autre relève la complexité du sujet.

Toute la question des rôles et responsabilités reste également floue du fait que nous devons taire le nom des institutions et des personnes. Mais il ressort que les risques sont gérés par des instances très variées d'une organisation à l'autre et que les noms utilisés pour les désigner sont aussi différents.

4.2 Définition du risque

Les archivistes ne peuvent pas fournir une définition du risque, mais leur vision du risque renvoie à leur travail de gestionnaire de l'information et donc du risque informationnel. Quatre répondants sur cinq s'accordent à définir le risque en fonction de sa probabilité d'occurrence et de son impact. Les définitions proposées rejoignent celles que l'on trouve dans la littérature et semblent assez officielles. Elles apparaissent sur le site internet des organisations ou sur l'intranet. Elles semblent toutes produites par l'organisation ou l'autorité de tutelle.

4.3 Définition du risque informationnel

L'institut de recherche et d'enseignement lie le risque informationnel à la sécurité de l'information et propose deux définitions de cette dernière où apparaissent les notions d'intégrité, confidentialité et disponibilité. Les autres disent qu'ils n'en ont pas ou n'en connaissent pas et donnent plutôt des exemples. Une archiviste dit qu'elle ne sait pas trop comment définir le risque informationnel, que c'est implicite, car cela renvoie à son travail quotidien.

Personne ne s'est vraiment longuement interrogé sur la définition du risque informationnel. Il est généralement compris comme un risque qui impacte ou a des conséquences fâcheuses sur l'information ou les actifs informationnels et non comme l'information qui est source de risque. Seul au DS, nous avons la mention de la communication mensongère, d'échanges d'informations sources de problèmes.

4.4 Qualités de l'information

L'information reçoit de nombreux qualificatifs en fonction des milieux et des idées personnelles des gens. L'information est sensible et confidentielle pour l'archiviste de HOP; elle a une valeur intrinsèque ou une valeur subjective dans le domaine de la recherche et de l'enseignement. Au sein du DS, l'information doit être d'actualité et référencée pour être utile et traçable : le cycle de vie de l'information est problématique ou plutôt la durée de conservation de l'information est délicate, le taux de récidive des délits invite à conserver les documents plus longtemps que nécessaire, car il en va de la sécurité des citoyens. La consigne est de la garder tant qu'elle est utile au policier, ce qui reste vague. Il y aussi la question de la véracité de l'information. Au niveau de la banque, l'information a une valeur de travail, une valeur légale, contractuelle, corroborative et a un niveau de confidentialité variable. Les documents sont traités différemment selon ces critères. L'information a aussi été qualifiée de privilégiée pour les employés qui peuvent l'exploiter en vue de faire du bénéfice. Elle est sensible, délicate. Elle est l'asset essentiel et ne doit pas être disséminée, elle a un coût. Les moyens investis sont énormes en termes de personnes, informatique ou contrôles. La loi et les règlements doivent être respectés et l'information doit être juste. Les banquiers parlent aussi des données live (des données opérationnelles, actives, vivantes) et des données d'archives, deux choses différentes dont ils doivent s'assurer de la sécurité.

4.5 Définition du patrimoine informationnel

Le patrimoine informationnel des diverses organisations correspond logiquement à leur domaine d'activité auquel on ajoute les documents administratifs. Dans plusieurs milieux, la documentation est sensible et il s'agit de la protéger. A HOP, il y a avant tout les dossiers des patients. Dans l'organisation internationale, c'est l'information liée à la spécialité de l'Organisation. Au DS, il y a surtout les documents liés à la police et à la sécurité. Pour l'établissement de recherche et d'enseignement, nous n'avons pas vraiment de réponses, car le responsable SI ne peut parler que de son secteur d'activité et là, il n'y a pas d'inventaire du côté de la sécurité, pas de listes d'actifs à protéger. Les banquiers ne répondent pas vraiment à la question. Comme une banque ne fabrique rien, ils disent que leur asset essentiel est l'information : l'information des clients, des affaires qu'ils gèrent. Dans le profil organisationnel de la banque, nous apprenons que la mission de cette banque est la gestion de fortune et des actifs des particuliers et des institutions. C'est un patrimoine pécuniaire. Nous constatons que certains répondants n'ont pas bien compris ce que nous entendions par « patrimoine ou actif informationnel ».

4.6 Identification (typologie) et classement des risques

Les gestionnaires de risques connaissent les risques de leur organisation et les classent directement dans des catégories. Identification et classement ne font qu'un. Les archivistes ne connaissent pas les catégories de risques. Ils citent des risques qui leur viennent à l'esprit et souvent ce sont des risques informationnels (cf. chap. 5.2.2). Par rapport à la revue de la littérature, nous constatons d'emblée que la gestion des risques est l'affaire surtout de professionnels du risque. De nombreuses catégories de risques sont mentionnées dans nos interviews. Dans l'institut de recherche et d'enseignement, c'est l'audit interne qui produit un manuel de référence des risques où figurent 7 catégories de risques : risques financiers et économiques ; risques juridiques ; risques matériels, techniques et élémentaires ; risques liés aux personnes et à l'organisation ; risques liés aux technologies et aux sciences naturelles ;

risques sociaux et politiques ; risques environnementaux et écologiques. Les risques sont revus chaque année dans chaque unité, chaque département et sont supervisés par la direction. A côté de ces 7 catégories, cette institution doit faire face à de nombreux risques techniques. Ceux-ci ne sont pas gérés de manière globale par l'institution, ils sont traités à part par le service de notre répondant ou le comité de sécurité informatique. L'approche de ces derniers était d'aller chercher les risques techniques qu'ils pouvaient avoir et ils les ont classés en 26 catégories. Pour ces risques, ils ont une autre classification.

L'OI a un guide de référence « Politique de gestion des risques institutionnels » qui mentionne un registre des risques à part. Le répondant parle d'un outil de management des risques développé pour répertorier tous les risques. Ce sont les risk manager des départements qui identifient et traitent les risques. Il y en a 6 catégories : risques financiers ; risques politiques/liés à la gouvernance ; risques d'atteinte à la réputation de l'Organisation ; risques liés au personnel/aux systèmes et aux structures ; risques stratégiques ; risques techniques/pour le domaine de spécialité de l'organisation et 42 « areas » ou sous-catégories.

La banque a 3 catégories de risques gérés par les risk managers qui rencontrent les responsables d'équipe et en discutent. Cette approche « bottom-up » est complétée par une approche « top-down » où le département qui chapeaute tout le groupe essaie d'imaginer encore d'autres risques. Ces trois catégories sont les risques opérationnels, de contrepartie et de réputation. Les risques opérationnels englobent tout ce qui est lié à l'information, à la fraude, tout ce qui peut être lié à des manquements en termes de confidentialité sur les problématiques d'intégrité de données et d'organisation. En cours de discussion, le risque humain a été évoqué et il entre dans cette catégorie. Il y a l'erreur humaine ou l'acte malveillant, appelé dans certains cas le délit d'initié. Le risque lié aux nouvelles formes de communication via le cloud et les réseaux sociaux a aussi été évoqué ici. Les risques de contrepartie concernent la relation avec les partenaires, clients et échanges avec leur situation financière. Le risque de réputation peut découler d'un problème dans les autres catégories.

A HOP, les quality officer vont voir les différents métiers et posent des questions aux gens du terrain comme à l'archiviste par exemple, ils établissent une cartographie des risques qui est mise à jour chaque année selon la méthode de l'Etat. Elle est institutionnelle avec une déclinaison départementale. La typologie du classement des risques est secrète. Au DS, le travail d'identification et classement des risques est fait par l'instance qui chapeaute les risques. Ils appliquent une politique qui est commune à l'Etat pour une gestion des risques en lien avec les activités, les métiers. Chaque service a des risques propres en fonction de son activité métier. Les personnes de cette instance signalent à l'archiviste un risque métier suite à un audit ou à l'établissement d'un tableau des risques. Le répondant mentionne ensuite des risques standards en lien avec l'implication, la responsabilité, des risques organisationnels, métier, de fraude, corruption, au sein des équipes.

Si les données n'étaient pas confidentielles, il aurait été intéressant de relever les différentes appellations des services ou des responsables qui s'occupent des risques et des différentes approches pour identifier les risques. La question des rôles et responsabilités aurait été pertinente ici.

4.6.1 Place du risque informationnel parmi les divers types de risques

Le risque informationnel n'est jamais évoqué comme type ou catégorie de risque. Tous nos répondants disent qu'il est disséminé parmi les autres risques. Dans l'OI, on peut trouver des

risques informationnels dans les 42 sous-catégories. Dans l'IRE, le répondant n'a pas une vue sur les 7 catégories de risque de l'institution, il connaît les 26 catégories de risques techniques et dit qu'il y a là aussi une petite partie consacrée à l'information. Pour le répondant du DS, le risque informationnel n'est pas établi, il est en lien avec la tenue des dossiers, la gestion de l'application métier, la gestion des droits et de la sécurité informatique ou la sécurisation des données. Dans ces trois dernières organisations, on voit qu'information et informatique sont souvent mises en relation. A la banque, le risque informationnel entre dans les risques opérationnels. Dix principaux risques sont sélectionnés et dans ce top 10, il y en a qui sont directement ou indirectement liés à l'information et aux données.

Aucune des cinq organisations ne traite le risque informationnel de manière transversale comme l'institution financière Desjardins dont nous avons parlé dans la revue de la littérature, mais les banquiers que nous avons interrogés imaginent qu'il est tout-à-fait possible de le traiter de cette manière à l'ère du digital où l'informatique et l'information sont utilisés avec beaucoup de procès automatiques, et que, en fait, les risques informatiques et les risques informationnels pourraient tous les deux être traités de manière transversale.

4.6.2 Types de risques informationnels

Les archivistes ont pu répondre aisément à cette question. A la banque, les 3 intervenants ont tous fourni de nombreuses informations. Dans l'IRE, le responsable des risques informatiques n'a pas pu citer de risques informationnels, mais il cite ailleurs les pertes de données qui sont lourdes de conséquences du point de vue financier, administratif ou lorsqu'il y a des brevets à la clé. Le répondant de l'OI a montré une dizaine de risques informationnels parmi les sous-catégories. Il parle de l'importance des risques de l'information dans les directives ou conseils techniques et propose de contacter *l'information security officer* IT pour plus d'informations. Il relie souvent le risque informationnel au cyberrisque et à la sécurité des SI. Dans le milieu de la banque, la culture du risque est très développée, les documents sont très sécurisés en termes de droits d'accès et pour éviter leur perte une fois qu'ils font l'objet du records management. On retrouve aussi plus vite les documents mal classés avec les systèmes de recherche informatisés. Les e-mails pourraient toutefois présenter une faille, ils sont stockés, mais ne sont pas archivés. Ce sont des données non structurées, difficiles à contrôler et à retrouver. Les données de travail se mêlent aux données personnelles. Il faut éviter la perte de documents importants, mais l'accès aux messageries électroniques individuelles n'est pas légal.

La perte ou fuite d'informations est le seul RI mentionné par tous. Il est considéré comme le risque le plus important par le répondant de la sécurité et le records manager de la banque.

Un tableau qui recense les risques informationnels cités dans les entretiens est présenté dans l'annexe 8.

4.6.3 Classement des risques informationnels

Comme le risque informationnel n'est pas clairement identifié, il n'y a pas de classement de risques informationnels.

4.7 Evaluation des risques informationnels

Comme les risques informationnels ne sont pas nommés expressément, ils ne sont pas évalués en tant que tels non plus. Nous avons peu d'informations sur l'évaluation des risques

en général, c'est un sujet confidentiel. Les gestionnaires de risques ne s'expriment que de manière laconique sur les matrices et les échelles utilisées, mais deux sur trois révèlent le nombre de risques traités. Les archivistes, eux, ne connaissent pas la gestion des risques de l'entreprise, ce n'est pas leur métier. Mais dans l'ensemble, l'évaluation du risque se fait comme nous l'avions vu dans la revue de la littérature.

À HOP, c'est la probabilité x le degré d'impact qui donne la gravité du risque et qui indique s'il faut vraiment agir ou non, s'il faut juste être attentif ou clairement prendre des mesures.

Au DS, l'archiviste dit qu'il y a deux aspects : des risques évalués de manière globale et des risques dans les projets informatiques. Les risques les plus importants sont liés à la gestion de la confidentialité ou à la production d'une prestation aux clients. Pour l'évaluation globale des risques du département, il nous a été proposé de contacter l'instance qui s'en occupe.

Dans l'IRE, il y a 7 types de risques gérés de manière globale, auxquels on ajoute les risques techniques. Le responsable dit qu'il fait du ISO 27005 à haut niveau. Les risques sont hiérarchisés, classés suivant leur impact et des échelles qualitatives sont utilisées. La probabilité d'occurrence des risques est traitée avec une matrice colorée comme nous l'avons vu dans la recension des écrits. Pour les risques techniques, l'impact est difficile à définir et la probabilité d'occurrence est impossible à déterminer, elle est transformée en fréquence. Notre répondant s'est aussi efforcé de redéfinir la menace, l'impact, les conséquences en arrivant au poste, il utilise aussi la notion de vulnérabilité.

A l'OI, ils ont développé un outil de gestion de risques où tous les risques et les traitements de risques sont relevés. Ils classent les risques par criticité ou gravité en fonction de leurs notes d'impact et de probabilité combinées.

A la Banque, les risk manager font l'inventaire des risques dans leur domaine et les évaluent sur une échelle d'impact et de probabilité. A cela, ils ajoutent l'ensemble des contrôles qui ont pour but d'atténuer ce risque, ce qui donne à la fin le risque résiduel, le risque net. Ils ont l'impact financier, l'impact réputationnel et l'impact appelé « autre », qui est souvent le travail supplémentaire pour corriger le risque qui s'est matérialisé. Il leur arrive aussi d'évaluer un risque cible qu'ils expliquent ainsi : « aujourd'hui on a un tel niveau de risques, compte tenu de tout ce qu'on met en place et on aimerait peut-être dans douze mois, dix-huit mois être à un niveau meilleur, donc on peut aussi pour chacun des risques indiquer quelle cible on veut atteindre dans un délai donné ».

4.7.1 Fiche de risques, description de risques, scénarios

Les archivistes à HOP et à la sécurité pensent que des descriptions de scénarios de risques se font. Le gestionnaire des risques du lieu de recherche et d'enseignement dit qu'ils n'ont pas de fiches par risque, mais un tableau global avec tous les risques. Ceux-ci ont un intitulé court et une description courte, un mini-scénario. Si le scénario est long, les collaborateurs se focalisent sur ce cas précis, cherchent une solution pointue et oublient le risque de base. Dans l'OI, le personnel est encouragé à remplir l'outil de risques, avec les scénarios. Les descriptions précises permettent d'évaluer de manière appropriée le degré d'exposition au risque. On précisera que cette organisation traite plus de 2800 risques alors que l'établissement de recherches a moins de 20 risques globaux et une centaine de risques techniques. A la banque 10 risques sont décrits.

4.7.2 Périmètre

Les risques informationnels sont-ils appliqués à l'ensemble de l'entreprise ou seulement dans un périmètre bien défini ? C'est une question sans vraiment de réponses ou sans les réponses que nous attendions du moment que le risque informationnel n'est pas reconnu et que des acteurs aux fonctions bien différentes s'expriment. L'archiviste de HOP donne un bon exemple de transversalité, elle évoque la confidentialité des données qui ne touche pas que son secteur et qui a aussi été évoquée par d'autres, le personnel a été sensibilisé à ce thème. Dans la revue de la littérature médicale, on constate aussi que c'est un thème majeur traité surtout en rapport avec les dossiers patients. A la sécurité, les risques informationnels doivent être en lien avec une activité métier, dit le répondant. Il dit plus loin qu'il serait absurde qu'il gère seul le risque informationnel, pour avoir plus de force, il faut gérer les risques dans leur ensemble. Dans l'institut de recherches, le responsable des risques parle du périmètre géographique ou physique touché par un risque informatique, les installations de même que les informations véhiculées sont touchés diversement suivant le risque. A l'OI, le risk manager dit que n'importe qui peut définir un risque informationnel, mais que ce serait plutôt les gens qui travaillent avec l'information qui le feraient. A la banque, tout ce qui est lié à l'information que ce soit des données vivantes, actives, opérationnelles ou des données d'archives "est géré correctement", disent-ils, leur sécurité est assurée tout au long de la chaîne de traitement.

4.8 Traitement, mitigation des risques informationnels

La banque évalue ses risques selon une échelle de probabilité et d'impact avec un contrôle mis en place pour atténuer les risques connus jusqu'à arriver aux risques résiduels. Dans l'institution de recherche, on priorise les risques, définit les mesures à mettre en place et on fait le suivi de l'implémentation. L'OI a un processus ascendant (*bottom-up*) d'évaluation des risques dans chaque secteur associé à un mécanisme qui les renvoie à l'autorité chargée de l'approbation qui décidera de la mesure de mitigation selon un processus descendant (t*op down*), il cite deux types de risques qui ont différents seuils de tolérance : ceux liés à la conformité (politiques, procédures, statuts, règlements administratifs, financiers et autres) ont un faible niveau de tolérance, tandis que les risques stratégiques et opérationnels sont plus tolérés afin de pouvoir relever les défis qui se présentent et continuer à avancer dans leur mission. Cela nous renvoie au risque perçu comme opportunité dans la revue de littérature.

Les archivistes cantonaux ne s'occupent pas directement de cet aspect et ne pouvaient donc pas nous répondre. Pour les deux, il s'agit plutôt de détecter les risques et les communiquer au département qui s'en occupe.

Les mesures de mitigation font partie de la gestion des risques dans toutes les institutions interviewées. Pour le traitement global, cela rejoint ce que nous avons trouvé dans la littérature (choix de traitement du risque selon niveau de gravité), ces mesures sont décrites dans des manuels et outils internes auxquels nous n'avons pas accès.

Un tableau avec les mesures de mitigation citées aux entretiens est disponible dans l'annexe 9.

4.8.1 Éviter la perte

Pour éviter la perte d'informations ont été cités : la protection des locaux, la documentation des mouvements (traçabilité), les garde-fous sur les systèmes d'information, l'identification de l'utilisateur, le paramétrage du logiciel de Records management, et aussi l'assurance « que le

personnel a accès à ces informations » (OI) que l'on traduit par la communication et sensibilisation du personnel.

4.8.2 Utilisation d'un Disaster Recovery Plan

A HOP, il se trouve au niveau de l'Institution et c'est obligatoire ; au niveau départemental cela est en train de se mettre en place. Aux archives du DS, il n'y en a pas ; si un souci arrive, un autre secteur sera contacté et s'en chargera. L'OI nous a conseillé de consulter l'IT et nous n'avons pas de réponse de la Banque. L'IRE affirme en avoir plusieurs, ils sont confidentiels pour réduire le risque de sabotage.

4.8.3 Externalisation

Presque tous font appel à un service d'externalisation soit dans le cadre du service ou de l'organisation. Le DS y fait recours pour le développement informatique et le transport des détenus ; à HOP, c'est pour le nettoyage ; dans l'IRE il s'agit de l'utilisation de Switch[6]. L'OI n'externalise pas dans le département gestion des risques, mais la sécurité des locaux est en partie externalisée. À la Banque, les archives et systèmes de records management sont entièrement à l'interne (archives physiques mais également base de données et serveurs), mais ils utilisent de plus en plus de services ou des applicatifs métiers, qui stockent des données à l'externe, souvent dans un cloud.

4.8.4 Monitoring, Audit, Suivi

A la banque, les risques sont évalués et mesurés par les incidents qui ont lieu. Ils sont présents dans les rapports et aussi discutés avec les employés dans leur évaluation annuelle. HOP mentionne un service d'audit avec les *quality officer* des différents départements. Le DS est à son tour contrôlé par un département de contrôle (monitoring, suivi d'indicateurs avec des répondants dans chaque entité), et par un service d'audit interne et un externe (pour contrôle, surveillance et problématiques liées à la transparence). L'IRE a un audit interne et un externe (qui peut être annuel, bisannuel), les risques techniques sont suivis « à la main » avec le comité de sécurité informatique et les autres risques sont suivis par la direction et on les suit aussi à la main. Il dit : « Pas les moyens pour un monitoring automatique » (argent, environnement technique complexe). C'est le seul interviewé qui ait pensé à nous parler de la façon utilisée pour monitorer les risques. L'OI a un monitoring en place, mais pas d'audit.

4.9 Normes et lois

4.9.1 Lois

Quelques lois trouvées dans la revue de littérature sont effectivement mentionnées : La loi cantonale pour la protection des données du canton en question est citée par tous les interviewés, à l'exception de l'OI. Celle-ci a mentionné les lois liées à la cybersécurité, à l'informatique et au Cloud et nous a suggéré de contacter l'IT pour les voir plus en détail.

Tout ce qui est décidé dans les services cantonaux est régi par la législation cantonale respective ainsi que la LArch. Certains domaines ont des règlements, des directives internes très spécifiques, comme le domaine financier ou les Organisations Internationales. Dans les

[6] Fondation Suisse qui fournit le réseau Internet aux universités

départements cantonaux, nous avons vu que des lois métier s'ajoutent aux divers règlements en place.

La protection de l'information touche une multitude de domaines à la fois : juridique, économique, technique, organisationnel, etc. Chacun de ces domaines a ses propres lois, normes et réglementations que l'on ne pourrait pas citer de manière exhaustive dans ce travail. Ainsi, il y a des lois qui traitent de la protection des données ou de l'information à plusieurs niveaux dans une entreprise et, comme cité par deux interviewés, elles peuvent être en conflit et varier d'un pays à l'autre.

> *« (...) quelle loi appliquer, garder l'information mais jusqu'à quand ? C'est clair qu'ayant des domaines avec des données sensibles (...) c'est compliqué. On n'a pas forcément toujours de réponse sur les délais de conservation parce que la loi sur les dossiers de [tel métier] dit : « tant que c'est utile (...) » l'utilité elle est vague (...) [entre le] droit de l'oubli [et] l'application des lois, qu'est-ce qui prime ? »* (DS)
>
> *« En tout cas, il y a vraiment des chevauchements, des contradictions entre les réglementations. »* (B)
>
> *« Tout l'enjeu c'est de réussir à trouver un juste milieu qui soit raisonnable ou de choisir où on va mettre notre appétit au risque parce que des fois il n'y a pas moyen de faire autre chose. »* (B)

Les lois mentionnées dans les entretiens se trouvent dans l'annexe 10.

4.9.2 Normes

En ce qui concerne les normes, aucune institution n'est certifiée avec les normes ISO relatives à l'information, cependant trois sur cinq s'en inspirent dans la pratique du métier. Les normes ISO 15489, série ISO 27000, ISO 27005 et normes AFNOR ont été citées.

4.9.3 Politique

Aucune institution n'a de politique spécifique pour les risques informationnels. La politique concerne la gestion des risques en général. Dans trois organisations, une politique des risques est en place et communiquée via l'Intranet. Il existe des formations, la mise en place de programmes, des notes d'information ou de sensibilisation. Au DS, la politique de gestion de risques n'est pas communiquée, vu qu'elle « se fait par niveau ». A HOP, la politique est communiquée de façon partielle aux personnes concernées pour éviter la fuite d'informations.

4.10 Logiciels, outils

Aucun logiciel n'est utilisé pour la gestion spécifique des risques informationnels. Comme déjà mentionné, ceux-ci sont traités dans la masse des risques sans être spécifiés.

Seuls trois logiciels ont été mentionnés dans les interviews : SAP (logiciel de comptabilité) et GRC (module de gestion des risques) pour la Banque et le logiciel de gestion des risques online de l'OI, où chaque personne autorisée peut insérer des risques identifiés dans le classement préétabli (il y a un champ "autres") ainsi que les propositions de mesures de mitigation. Il est adapté aux besoins de l'organisation et a été fait suivant son Code de bonnes pratiques en gestion des risques.

Les outils pour la gestion des risques consistent essentiellement en : registre ou référentiel des risques, grille, logigrammes, processus, bases de données, cartographie des risques mise à jour annuellement, normalement institutionnelle avec une déclinaison départementale dans

les institutions publiques. Il a été mentionné que le contenu traité par ces outils n'est pas un document public dans les départements cantonaux. Dans un service cantonal, il a été mentionné « qu'il n'y a pas de méthode particulière autre que les bonnes pratiques du métier, bien connaître les procédures » (HOP), dans une autre institution publique la méthode n'était pas connue (DS). L'IRE utilise Excel comme outil, un autre serait trop cher à acquérir.

4.10.1 Calendrier de conservation

Tous utilisent un Calendrier de Conservation. Rien n'a été mentionné à ce propos par l'IRE mais vu que le répondant a cité la Loi sur l'archivage, cela laisse entendre qu'il doit y en avoir un. Le DS a aussi cité l'existence de « métadonnées qui reprennent certains délais ».

D'ailleurs, le conflit des lois pour le délai de conservation a été mentionné dans cette partie de l'entretien (DS et B).

4.10.2 Manuels de référence

À HOP, le manuel c'est la méthode de l'Etat qui est sur internet.

Le DS et la banque n'en mentionnent pas. La banque a une politique des risques et toute sortes de directives internes.

L'OI a un guide de référence, une « politique de gestion des risques institutionnels ».

Dans l'IRE, l'audit interne produit un manuel de référence des risques. Il s'agit d'un ensemble de feuilles agrafées. Il est confidentiel. On y retrouve les catégories de risques, les dimensions qu'ils prennent en compte pour mesurer les impacts et les probabilités d'occurrence des risques.

Notre idée était de savoir si les organisations utilisaient des manuels de référence, voir des ouvrages de chercheurs pour le classement des risques. En fait, elles utilisent plutôt des brochures ou des documents de référence conçus en internes et ceux-ci sont confidentiels. On n'en connaît pas vraiment le contenu. Ces documents peuvent contenir la politique en matière de gestion des risques. On ne sait pas si s'ils sont basés sur des théories de chercheurs.

4.11 Rôles et responsabilités

Dans les cinq institutions interviewées il était clair que la gestion des risques prend une place importante dans l'organigramme, qui irait, si on cite Lacroix (2007), de « l'organisation globale » à « l'organisation centrale réduite » (p.20), la gestion des risques étant directement liée à la direction.

Le risque informationnel est traité comme les autres risques, mais il est difficile de saisir qui les gère, le département qui s'approcherait le plus serait le département de sécurité de l'information, plutôt associé à la gestion informatique, et qui se situe dans l'organigramme au même niveau que le RH ou le département des finances. N'ayant pas pu avoir accès aux organigrammes de toutes les institutions, en plus de l'anonymat de certaines interviews à respecter et devant l'impossibilité de trouver un responsable pour les RI, nos conclusions sur cette partie ne peuvent être que partielles.

Il semble qu'à la Banque, la gestion de tout ce qui concerne l'information est très réglementée puisque pour le bon déroulement des activités il faut respecter les lois, vu que le cœur de ce

domaine réside dans l'information traitée (valeurs, noms, stratégies). C'est un domaine à la fois très spécifique et très formalisé qui touche le droit, l'éthique, la technique et la stratégie. Une petite perte d'information dans une banque pourrait nuire rapidement à sa crédibilité. D'ailleurs, c'était la seule institution qui a proposé de répondre à l'interview avec la collaboration de trois personnes-clés pour la gestion des risques de l'information.

Dans les autres institutions, il existe des départements qui travaillent plus directement avec la gestion de l'information que d'autres, ce sont des organismes plus compartimentés et avec des départements qui ont chacun leurs spécificités. Les risques (RI inclus par conséquent) sont traités avec une approche plutôt orientée métier. Ainsi, il y a normalement un département qui s'occupe des risques en général, et qui communique avec des intermédiaires qui sont des représentants dans chaque secteur (ex. HOP : le Responsable de secteur parle au *Quality Officer* de son département et celui-ci traduit les problèmes dans la grille).

L'Organisation Internationale a un outil qui permet à tout collaborateur ayant accès d'insérer un risque trouvé, mais la déclinaison du risque en métiers et départements reste présente : « In the kind of case of people whose mandate is really information management, the criticality of these risks would be quite a lot high for them. So I think it's very much derived from what the unity or the department is supposed to do, if it's close to information management this risk could be higher. »

Les approches de gestion des risques sont décrites comme étant à double sens dans la Banque et l'OI : bottom-up et top-down, qui seraient complémentaires. Selon le niveau de gravité du risque il reste au niveau du département ou bien il est communiqué à la direction générale (OI, IRE).

4.11.1 Communication

Rouhier (2008) mentionne quatre acteurs principaux qui interviennent dans la protection de l'information : l'entreprise, la hiérarchie, les métiers et chacun individuellement. C'est pour cette raison que nous avons cherché à savoir comment le personnel est inclus dans la gestion des RI et comment on l' implique dans la démarche.

Nous avons pu constater plusieurs niveaux de communication des risques au personnel :

A la Banque, la sensibilisation des employés se fait régulièrement. Pour prévenir les RI, on communique les mesures de prévention via sensibilisation, présentations à l'auditorium. Pour vérifier si cette sensibilisation est efficace il y a des mesures qui sont faites régulièrement via le « rapport d'incidents, la détection des signaux faibles », ces mesures sont aussi inclues dans les objectifs des collaborateurs dans leur évaluation annuelle.

Dans les archives de HOP la sensibilisation des employés est aussi faite régulièrement. « Le Service juridique est très attentif en ce qui concerne la confidentialité des données ». La communication sur les mesures de protection de l'information sensible est faite. Par contre, il n'y a pas de mesures établies pour évaluer l'efficacité de la sensibilisation.

A l'OI, la sensibilisation des employés se fait par la mise en place de différentes politiques, programmes, notes d'information, intranet, training. Pour les risques informationnels spécifiquement, le répondant nous a suggéré de consulter l'IT.

Il y a des institutions où une culture du métier semblerait jouer un rôle dans la protection de l'information : dans l'IRE, pour le personnel administratif la sensibilisation aux RI est « intrinsèque au métier », à cela s'ajoute encore la distribution de fascicules de sécurité, emails et présentations. « Les RH sont sensibilisés aux notions de confidentialité et au principe de protection des données personnelles, aux finances, à la confidentialité, à tout ce qui est intégrité, traçabilité. » Par contre, du côté de la recherche, ce n'est pas encore tout à fait acquis : « ce n'est pas dans leur nature », dit le répondant. Exception faite pour « les brevets à la clé ou [si] une start-up va se monter à partir d'une découverte, les chercheurs ont tendance à bien faire attention et à se renseigner. » Pour sensibiliser les chercheurs, plusieurs actions sont menées : distribution de fascicules sur la sécurité, vidéos explicatives. Ils font de la sensibilisation par corps de métiers (ex. secrétaires). La mesure de l'impact de cette sensibilisation semblerait difficile car la population est très grande et variée, dit-il.

Dans le DS, la sensibilisation est faite « dans les grandes lignes, liée au secteur, de caractère plutôt préventif et jamais approfondi ». L'outil de gestion des documents est considéré comme suffisamment paramétré pour complémenter cette sensibilisation. Des informations, des directives, des pop-ups sont utilisés dans le département. Le répondant a mentionné qu'il partage parfois le matériel élaboré par le Préposé des Données.

5. Interprétation des résultats

5.1 Risque Informationnel

5.1.1 Le risque informationnel dans la gestion des risques

Le risque informationnel a pris de l'importance avec les évolutions technologiques et l'essor des médias dans l'entreprise à partir des années 1990 (Hassid, 2008). On le rapproche donc souvent des risques informatiques dans les écrits sur les SI ou des risques de réputation dans les milieux de la communication. Aujourd'hui, il semble aussi trouver une place dans la gestion des dossiers des patients ou des clients. On peut se poser la question de son statut que ce soit en théorie ou en pratique ; ce risque semble avoir de la peine à s'imposer. Dans la littérature, il fait l'objet d'études particulières, mais n'apparaît pas souvent dans les classifications proposées par les études en gestion des risques. Là, on trouvera des types de risques tels le risque naturel, humain, politique, technologique, etc.

En pratique ou sur le terrain, il est difficile de se prononcer avec notre échantillon de cinq organisations. Nos répondants disent connaître les risques informationnels, mais n'en font pas une catégorie. Un risque informationnel est souvent combiné à un autre type de risque (la mauvaise gestion des documents peut aussi être perçue comme un risque humain, par ex.) ou placé parmi les risques opérationnels ou internes qui constituent des catégories plus générales de risques. Nous ne savons pas si d'autres sociétés considèrent le risque informationnel comme type de risque, mais nous restons sur l'impression que ce n'est pas le cas.

La classification des risques en catégories est dans l'ensemble délicate, car tous les risques peuvent se combiner. Aussi, certains managers préfèrent lister une dizaine de risques importants propres à leur entreprise.

Les ouvrages particuliers sur le risque informationnel tels ceux de Lemieux ont le mérite de sensibiliser les entreprises à ce risque. Lemieux et Krumwied proposent qu'il soit considéré comme un risque à part entière pour qu'il soit évalué et traité efficacement (Lemieux et Krumwied 2011). Dans cette optique, on peut déjà lui accorder une place plus importante dans la cartographie existante des risques d'une entreprise.

Comme le risque informationnel ne touche pas que la gestion des records et les milieux de la communication, mais l'ensemble des activités et des unités d'une organisation, Lemieux et l'institution financière Desjardins (2011) proposent une approche globale de ce risque. Lemieux (2004b) propose des pistes pour sa réalisation pratique.

5.1.2 Types de risques informationnels

Dans la littérature, les risques informationnels sont listés ou regroupés dans des catégories. Ils sont souvent mélangés et confondus avec les risques informatiques, du fait que les moyens techniques ou informatiques véhiculent l'information ou sont souvent causes de risques informationnels. Certains, comme Eduscol (2015), disent qu'ils sont d'ordre technologique, humain, ou liés aux risques naturels. Certains les associent à la gestion de l'information comme l'Uniris (2016) ou à l'information-communication comme Harbulot (2005), ils sont là plutôt réunis thématiquement. Sur le terrain, seuls certains risques informationnels sont identifiés, mais au sein d'autres catégories.

Quels sont finalement les risques informationnels ? Il nous semble bon de relever ici ceux qui apparaissent dans la littérature et sur le terrain. Nous les regroupons de manière sommaire. Le terme « informations » couvre aussi les termes « données » ou « documents ».

1. Détérioration, destruction des informations, mauvaise conservation (volontaire ou non)
2. Erreurs et omissions dans la gestion et le classement des informations (conservation ou non conservation, délais à appliquer, gestion trop étendue des infos hors de la société)
3. Perte, fuite ou indisponibilité d'une information
4. Accès illégal ou non autorisé aux informations
5. Utilisation illégale ou abusive des informations (copie, modification, rétention d'informations)
6. Vol d'informations
7. Divulgation d'informations confidentielles
8. Diffusion d'informations fausses, mensongères
9. Interprétation erronée des informations
10. Manque de fiabilité, informations inutilisables (production ou réception d'informations erronées), informations décontextualisées.

Les risques informationnels ne sont pas nombreux, mais leurs causes sont innombrables. Faut-il, dès lors, chercher à les classer par thème, nature, causes, impact ou autre ? La classification permet peut-être de les repérer facilement, de désigner des responsables de risques, mais les classifications ont leurs limites. Il faut surtout que l'entreprise soit consciente de l'existence de ces risques. S'ils ne sont pas identifiés, ils ne sont pas gérés.

5.1.3 Standards, normes, bonnes pratiques et aspects juridiques

L'utilisation des données permet d'informer et créer de la connaissance. Ainsi, des données personnelles sont utilisées pour donner de l'information utile aux entreprises, pour tracer un profil exact de leur clientèle. En même temps, elles sont utiles à la recherche, aux études scientifiques (par ex. les analyses du profil génétique[7]). Ce sont deux aspects de la gestion du RI : risque et opportunité. Opportunité d'améliorer un service, de faire des progrès scientifiques, et, d'un autre côté, risque de fuite d'information ou d'une mauvaise utilisation de données récoltées.

Avec le choix de porter nos interviews sur cinq différents secteurs, nous avons pu constater que des normes et législations cadrent certaines procédures clés des métiers, gestions des risques informationnels inclus. Ainsi, la banque devra se plier aux nombreuses exigences juridiques qui touchent le domaine financier, « régies à la fois par le secret bancaire et les 39 articles de la loi fédérale sur la protection des données, les banques ont une activité très encadrée » (Farine et al. 2015). Les hôpitaux seront particulièrement attentifs aux données médicales : « Les données de santé sont par nature très personnelles et donc sensibles. En Europe, elles disposent d'un statut de protection parmi les plus élevés. Nous avons depuis mai 2016 dans l'Union une réglementation générale qui assure un cadre commun pour les données personnelles, avec un statut spécial, une protection renforcée pour les données de

[7] FARINE, Mathilde *et al.,* 2015. Comment les entreprises utilisent nos données. *Le Temps : TMagazine* [en ligne]. 28 décembre 2015. [Consulté le 3 avril 2017].

santé » (Goubet 2016). En Europe, l'entrée en vigueur du règlement général sur la protection des données (GDPR) en mai 2018 va consolider les droits des individus, exiger la protection accrue de leurs données (Knowckers 2017).

Dans la brochure "Protection du patrimoine informationnel" (Caprioli 2007) sont citées plusieurs lois qui touchent le risque informationnel, dont nous avons déjà présenté les principales dans la partie revue de littérature de ce travail. Il est intéressant de voir comment plusieurs aspects de l'information peuvent être couverts par la législation : pour se protéger d'un risque, pour s'assurer en cas de souci, mais aussi pour s'enrichir. A ce sujet nous avons aussi consulté Gagnon-Arguin et Vien (1998), mais les lois sont québécoises et le contenu de l'article porte exclusivement sur l'information de fonctionnement [8] Nous regrettons de n'avoir pas trouvé un document équivalent pour la législation informationnelle helvétique.

Selon le canton et la loi métier concernée, on trouvera plus ou moins d'articles concernant la protection de l'information. Ces lois sont appliquées comme nous avons pu le constater, mais elles peuvent être sources de conflit quand elles sont mises en parallèle (délais de conservation de documents, exigence de mise à disposition, etc.).

Les normes et les standards peuvent aussi se décliner selon le métier et ses spécificités. Elles ne sont pas forcément utilisées dans l'optique d'obtenir une certification. Quatre organisations interrogées sur cinq s'en inspirent, aucune n'est certifiée. Cela pourrait s'expliquer par le fait que, bien qu'elles consistent en un guide pour les « best practices », les normes demandent beaucoup de maintenance, sont coûteuses à gérer et présentent surtout un écart entre théorie et réalité qui peut les rendre difficiles à mettre en pratique (Smallwood 2014, p.77).

Plusieurs normes traitent la gestion de l'information dans ses multiples facettes. Il s'est avéré impossible de faire un travail exhaustif à ce propos : certaines normes vont traiter plutôt de l'aspect gestion de risque, d'autres de l'archivage papier et de son conditionnement, de l'externalisation, de l'archivage électronique, du records management, etc. Les référentiels abondent : normes, certifications, standards, français ou internationaux.

5.2 Entreprises et traitement des risques informationnels

5.2.1 État de la situation

Nous constatons un décalage entre ce qui est conseillé dans la revue de littérature et ce qui est fait dans la pratique. Sur le terrain, les risques informationnels sont traités dans les processus administratifs en fonction de chaque secteur. Ils sont dilués partout dans l'organisation qui les traite en fonction du danger qu'ils pourraient représenter. Après avoir été identifiés, les risques sont remontés pour analyse et traitement, et même si une approche à double sens (*bottom-up* ensuite *top-down*) est mentionnée, le processus reste très dissocié entre les secteurs eux-mêmes et au niveau global de l'entreprise.

Le terme « patrimoine informationnel » a posé problème dans certains entretiens. Pour nous il semblait évident que chaque organisme serait au clair avec ce concept, mais cela n'a pas été le cas pour tous. Il y a eu confusion entre les sens « héritage » et « bien propre » et nous avons dû le clarifier. Cette confusion serait-elle l'indice d'une méconnaissance de la valeur de capital qu'ont les documents gérés par le département/l'institution ?

[8] Voir le chapitre « 2.2.1. L'information dans l'entreprise »

La communication sur les risques informationnels est faite aussi par secteur, à travers des formations, l'intranet ou la sensibilisation. Elle existe, mais ne touche en général que les problèmes des secteurs concernés. Pour certains départements il y a encore une culture procédurière qui croit que, si les procédures sont suivies comme il faut, il n'y a pas besoin de sensibiliser les employés. Dans d'autres institutions, elle semble être plus globale et intègre des communications intranet ou messages directs dans les boites email des employés.

A l'exception des organismes qui ont l'intention de sous-traiter la gestion des données informatiques, l'externalisation n'a pas été mentionnée en tant que facteur à gérer. Il nous semble qu'il serait important de prendre en considération les risques liés à l'externalisation, quelle que soit sa nature (nettoyage, transport de détenus, service de sécurité le soir, etc.) par la limitation d'accès à certaines parties de l'entreprise ou par des clauses de confidentialité concernant les données qui circulent avec des prestataires externes.

5.2.2 Évaluation et traitement des risques informationnels

La gestion des risques est bien documentée et réglementée par des normes. Lors des entretiens, nous avons constaté que l'analyse des risques était l'affaire de professionnels, entre autres des gestionnaires de risques. Mais la gestion des risques est restée un peu obscure, car, pour des raisons de confidentialité, nous n'avons pas pu accéder aux registres des risques ou autres documents qui nous auraient permis de mieux cerner les méthodes et outils utilisés. Il s'avère que la réalisation de cartographies des risques est très variée et propre à chaque institution, mais toutes suivent plus ou moins les schémas et idées que nous avons présentés dans la revue de la littérature.

Les gestionnaires de risques faisaient référence aux méthodes de gestion des risques que nous avons trouvées dans la littérature, mais ne se sont pas penchés spécifiquement sur le risque informationnel. Nous n'avons pas pu voir d'exemples d'analyse de risques informationnels. Les archivistes, eux, ne connaissent pas la gestion des risques, mais connaissent bien les risques liés à l'information qu'ils traitent.

Avoir le point de vue des deux corps de métier est intéressant, car ils se complètent et notre perception du traitement des risques varie aussi suivant qu'il nous est présenté par l'un ou l'autre. Les archivistes traitent de nombreux risques de manière simple et concrète, par conscience professionnelle. Ils adoptent de bonnes pratiques quotidiennes et des mesures de sécurité comme, par exemple, l'interdiction de communiquer des informations personnelles par téléphone, toujours fermer les portes et les fenêtres. Les gestionnaires de risques, eux, évitent, réduisent, externalisent des risques d'une manière qui nous semble plus théorique, scientifique en tenant compte de la conformité, du coût et des conséquences des risques. Les archivistes ou records manager pourraient peut-être jouer un rôle de conseiller dans la gestion du risque informationnel au même titre que d'autres corps de métiers (ex. marketing, communication). Leur expérience est certainement utile, notamment au niveau de la réalisation d'outils de sensibilisation.

Dans notre idée de départ, nous pensions qu'il pourrait y avoir des différences dans l'évaluation et le traitement des risques selon le secteur d'activité de l'entreprise. Au vu des limites rencontrées dans notre collecte de données et le caractère fractionné du traitement des RI, nous ne pouvons pas vérifier si tel est le cas. Il nous semble, cependant, que le domaine des finances montre plus d'aisance dans la protection de ses actifs informationnels.

5.2.3 Rôles et responsabilités

Il ressort des entretiens que les risques liés à l'information sont éparpillés dans toute l'entreprise. Même si l'on sait qu'il y a des mesures de mitigation instaurées pour tout risque identifié, nous avons l'impression que le risque informationnel n'est l'affaire de personne en particulier : il n'y a pas de responsable avec une vision globale de la gestion de l'information dans l'entreprise. Nous avons été reçues soit par des risk managers soit par des archivistes (à l'exception de la banque où trois responsables sont venus) qui nous ont suggéré de contacter d'autres secteurs de l'entreprise qui seraient plus en mesure de nous donner des informations complémentaires. Il s'agissait généralement du service IT ou d'un département de conformité. Cela va de pair avec ce que dit Lemieux (2004b) : « Despite the risks of failing to manage them holistically and systematically, records and information risks are not recognized as a distinct area of focus in most organizations and, therefore, no processes or people are specifically dedicated to them. » (Lemieux 2004b, p.57)

Si on trace un parallèle avec les approches citées par Lemieux (2004b)[9], on peut dire que les organisations interviewées adoptent le traditionnel modèle « Event-based approach » :

> *« The traditional approach usually begins with a survey of the organizational environment to identify all possible sources of threats to records and information. The business impact of these risks is then assessed. (…) In most cases in a large organization, management assigns ownership of [the risk mitigation] strategies to particular groups or functional areas. For example, (...) IT security groups will focus on risks arising from breaches of computer security; and legal groups will focus on risks arising from laws, regulations, or litigation »* (Lemieux 2004b, p.59)

[9] Voir en « 2.9 : Deux approches »

6. Conclusion

6.1 Proposition d'un modèle de gestion des risques informationnels et de ses composantes

> *« En effet, l'information est un concept abstrait, une « chose » impalpable, et cependant multiforme donc difficile à saisir. De plus, l'information est quelque chose de transversal, de fugace : elle traverse sous forme de flux les différentes unités de l'entreprise (ou d'un organisme public), mais aussi ses frontières (plus que poreuses).»* (Lesca 2010, p.9)

Quand on prend en considération ce caractère mouvant de l'information, changeant selon son cycle de vie ou selon le point de vue du secteur qui la traite, on ne peut que conclure qu'il s'agit d'un sujet complexe et qui touche à l'entreprise dans sa globalité. Toute solution fractionnée et isolée par département ne permettrait qu'une vision partielle des problèmes et capacités de l'entreprise.

Pendant nos recherches nous avons trouvé une présentation donnée par Le Mouvement Desjardins (2011), un grand groupe financier coopératif au Canada. Cette institution applique ce qu'ils appellent la « gestion intégrée des risques ». Leurs risques « sont regroupés en 7 catégories autour d'un langage commun ». Dans cette approche les risques « sont traités dans une dynamique interrelationnelle et intégrés dans les pratiques de gestion et systèmes décisionnels ». Ils proposent un modèle de GRI (gestion de risque informationnel) qui est traité de façon holistique : le risque informationnel existe et fait partie de leurs risques opérationnels. Dans la gestion de leurs RI, ils mettent en avant les enjeux de l'entreprise et les objectifs qui en découlent. C'est de cette façon que les RI sont présentés : pour « gérer les risques associés à l'information de façon à atteindre des objectifs d'affaires » et « une opportunité pour revoir [leur] vision ». Pour cela ils travaillent sur « la clarification des rôles et responsabilités entre les différents intervenants » et intègrent « les pratiques avec les secteurs d'affaires et [établissent] un solide partenariat avec les fonctions de soutien (ex. TI, RH, gestion de projet, approvisionnement, contrôles internes, etc) »

L'approche adoptée par Desjardins nous semble être particulièrement en harmonie avec la nature complexe de l'information. Leurs risques sont évalués en partant de la définition des enjeux et objectifs de l'entreprise et ce de façon holistique. Les RI sont compris comme étant transversaux aux autres risques et ont une place dans la stratégie au niveau de la direction.

Suite à nos analyses, il nous semble que la démarche proposée par Desjardins (2011) et celle citée par Lemieux (2004b), « Records and Information Requirements-Based Approach » sont celles qui se rapprochent le plus d'une gestion efficace des risques informationnels. Pourtant cette dernière reste très théorique et ne semble pas avoir été mise en application.

Il y a une différence entre une stratégie défensive qui identifie les défaillances pour les attaquer et une stratégie basée sur des objectifs à atteindre. Quand on passe de la première perspective à la deuxième il est plus probable que les procédures mises en place soient orientées vers le développement, la créativité et la croissance, et pas uniquement l'évitement du problème. Lemieux (2004b) propose justement que les qualités que l'information doit avoir soient établies avant la liste des risques liés aux défaillances. Quand on pense à ce que l'on veut globalement pour une institution à partir de l'identification de ses besoins, on agit en conséquence et dans une attitude plus systémique. Or, l'information est transversale, et elle demande une gestion elle aussi transversale, qui l'accompagne dans ses flux et ses cycles.

Cela peut représenter un grand effort au début, mais le retour sur investissement en vaudra la chandelle. Il sera nécessaire de faire des changements dans l'organisation des tâches, de sensibiliser le personnel, et d'intégrer cette nouvelle approche dans la culture de l'entreprise. Le rôle des professionnels de l'information devra aussi être redéfini (Lemieux 2004b).

> *« In addition, roles and responsibilities for functional areas that have traditionally focused on records and information management or dealt with certain types of records and information risk, such as a records management department or the IT department, will need to be redefined in relation to how records and information risk management fits into the organization's enterprise-wide risk management program. »* (Lemieux 2004b, p.59).

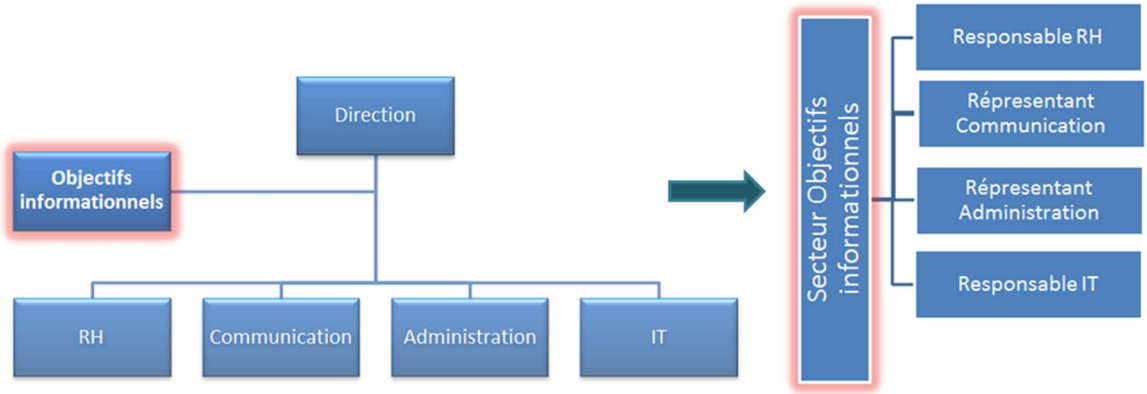
Les spécialistes de domaines traditionnellement liés à la gestion de l'information et de leurs risques tels que records managers, archivistes, spécialistes en TI, entre autres, pourraient jouer un rôle de conseiller ou de référence dans la gestion du risque informationnel.

6.1.1 Création d'un département dédié aux RI

La création d'un département dédié aux RI au niveau de la direction légitimerait l'importance de la bonne gestion de l'information. Il pourrait être intégré à un risque déjà existant (comme chez Desjardins, qui les intègre aux risques opérationnels qui font eux-mêmes partie d'une gestion intégrée des risques) ou constituer un secteur à part entière.

A notre avis, la meilleure option est qu'il soit un département à part entière. Ce secteur traiterait la gestion des objectifs informationnels de l'entreprise, et s'occuperait d'atteindre les objectifs informationnels préalablement recensés, en listant les qualités que l'information doit avoir dans chaque département. Pour que le caractère transversal nécessaire à une vision globale de l'information gérée soit présent, ce service serait constitué de personnes travaillant dans d'autres secteurs et qui connaissent bien leurs domaines et équipes, comme par exemple un responsable SI, un responsable documentaliste, un responsable au département juridique, RH, communication, ou autres, selon la configuration de l'institution. L'important étant que ce nouveau secteur soit intégralement représentatif de l'entreprise. Cela permettrait d'avoir une vision globale des actifs informationnels, de faire une gestion transversale des RI, de gérer plus rapidement et efficacement les défaillances ou saisir des opportunités tout en ayant une vision d'ensemble de cet organisme vivant qu'est l'entreprise.

Figure 9 : Département pour la gestion de l'information et ses risques



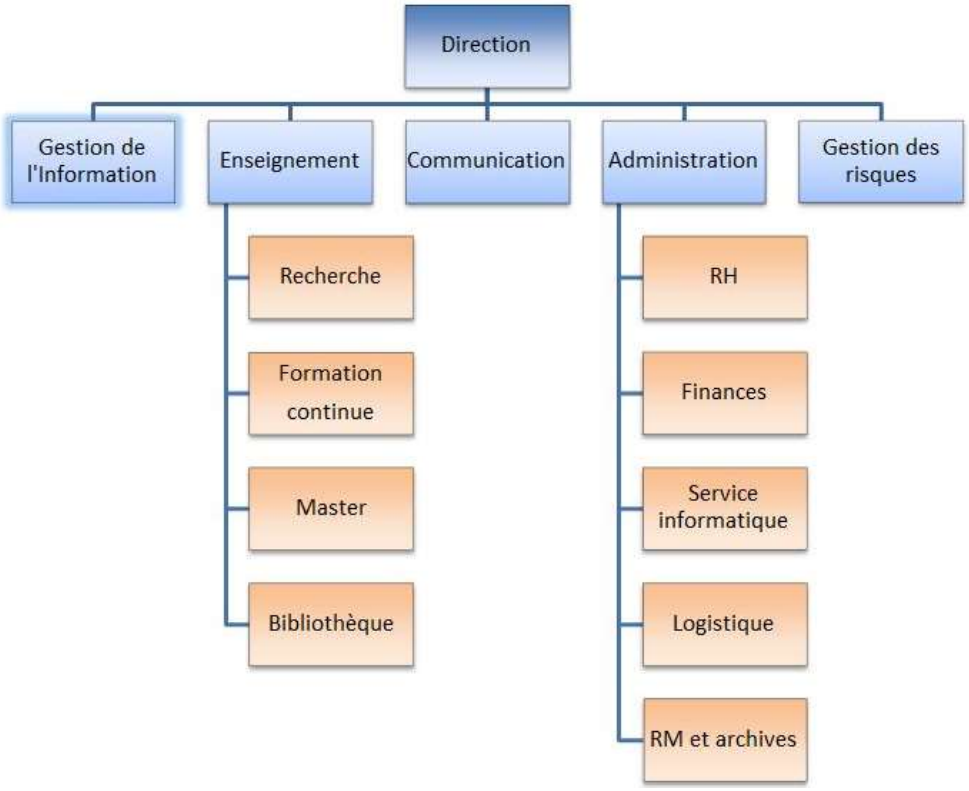
6.2 Cartographie des risques informationnels

Pour donner une vision plus concrète de notre proposition, nous avons préparé une cartographie des risques informationnels avec une approche de gestion transversale. Il est

clair que ce n'est qu'une suggestion et que c'est la réalité de l'entreprise qui dictera le contenu de chaque grille. Nous la fournissons en tant qu'exemple illustratif.

Nous avons imaginé un contexte fictif pour servir d'exemple. Il s'agirait de la cartographie des risques d'une école de management international. L'organigramme montre les secteurs rattachés à la direction. Parmi eux, le secteur « gestion de l'information ». Contrairement aux archives, RM ou à la communication, le secteur a des objectifs spécifiques qui regroupent les besoins informationnels de l'institution dans sa globalité. Ainsi, il est constitué d'un directeur de gestion de l'information, d'un responsable de chaque secteur en bleu et d'un représentant de chaque département en orange. Des réunions mensuelles permettent de faire le point sur l'atteinte des objectifs programmés ainsi que des problèmes à gérer. Pour établir ses objectifs, cette institution se base sur une liste de qualités de l'information[10] et le sujet est largement communiqué à tous niveaux. Chaque département choisit les 4 plus importantes qualités qui seront des objectifs à court et long terme. Des rapports semestriels font un bilan de la situation.

Figure 10 : Organigramme de l'institution



[10] Voir liste de Dietel 2003, p.44-51, aussi très bien résumée par Lemieux 2004b, p.60

Figure 11 : Cartographie des RI : une approche transversale

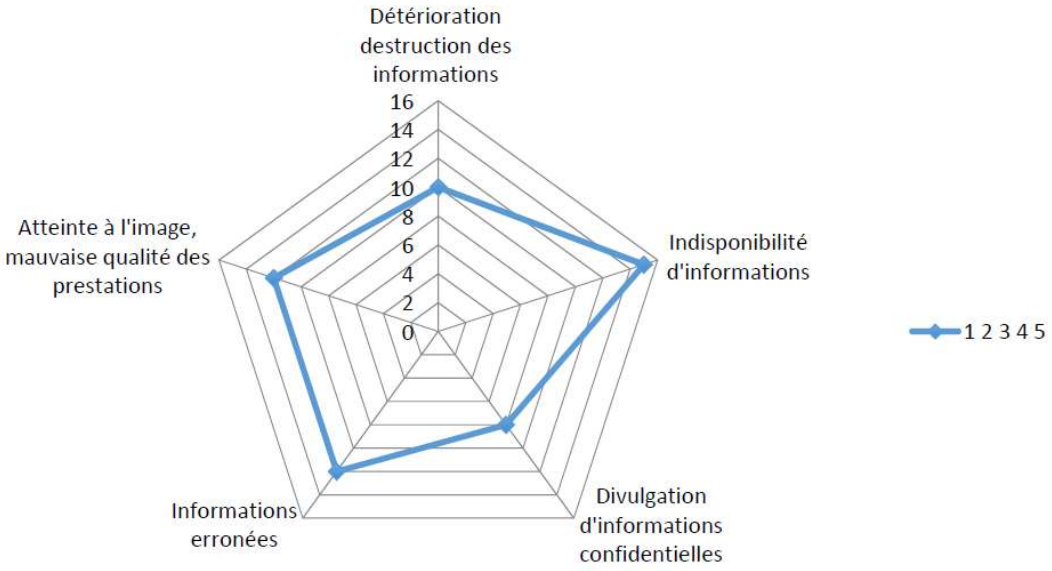
Cartographie des Risques informationnels en approche transversale

Objectifs de l'information									Services ou départements concernés					Risque No	Titre du risque	Détail, description du risque	Causes	Mesures	Probabilité *	Impact **	Score	Traitement					Responsable du risque
Intègre	Disponible	Confidentielle	Communicable	Partageable	Engageante	Pertinente	Complète	Utile à l'avenir	Direction	Enseignement	Communication	Administration	Gestion des risques						(1à 5)	(1 à 5)	(prob.*imp.)	Ignorer	accepter	réduire	éviter	transférer	M. / Mme ..
x	x	x	x					x				x		1	Détérioration, destruction des informations	Mauvaise conservation des archives	Locaux inadaptés, présence de rongeurs	Contrôles hygrométrique, sanitaire et incendie	2	5	10			x			
	x		x	x			x		x	x	x	x	x	2	Indisponibilité d'informations	Indisponibilité d'informations au moment opportun, information incomplète	Mauvais rangement des dossiers, mauvaise entrée des données, problèmes techniques	Sensibilisation, mise en place GED, RM, sécurisation des SI, veille,etc	5	3	15			x			
		x							x	x	x	x	x	3	Divulgation d'informations confidentielles	Divulgation de données personnelles, des données stratégiques	Facteur humain (volontaire ou non), erreur technique	Sensibilisation, prévention, sécurisation des SI	2	4	8			x			
x						x		x	x	x	x	x	x	4	Informations erronées	Données financières erronées, erreur de paramétrage du SI, données des étudiants et du personnel inexactes	Facteur humain (volontaire ou non), erreur technique	Sensibilisation, prévention, paramétrage correct des SI	4	3	12			x			
x			x	x	x	x			x	x	x	x	x	5	Atteinte à l'image, mauvaise qualité des prestations	Indisponibilité des outils pour l'apprentissage	Outils pour l'accès et le partage d'information indisponibles ou pas satisfaisants (PC, réseau, imprimantes, scanner). Ressources limitées dans la bibliothèque (base de données, livres)	Contrôle du bon fontionnement des outils. Investissement dans le fonds de la bibliothèque. Veille réputationnelle active et présence dans les réseaux sociaux.	3	4	12			x			

Pour une meilleure lisibilité, cette cartographie est disponible à l'annexe 11.

Pour avoir une vision globale de l'urgence des risques à traiter nous proposons un radar des risques. Ceux qui touchent le bord sont à traiter avec priorité :

Figure 12 : Radar des risques



6.3 Conclusion

Il reste beaucoup à chercher et à produire au sujet des risques informationnels. Si nous poursuivions ce travail, nous essayerions de clarifier les rôles et les responsabilités dans la gestion des risques, de savoir quel département gère quoi. Même en sachant que cela dépend de la structure propre à chaque entreprise, nous pensons que des faits intéressants pourraient être soulevés.

Nous essayerions également d'élargir la quête à d'autres approches pour le traitement des RI, mais surtout de trouver des entreprises qui utilisent un modèle autre que le traditionnel « event-based approach » (Lemieux 2004b), afin de voir comment les RI sont pris en compte dans leur contexte et quels résultats en sont tirés.

Il serait aussi intéressant de savoir comment d'autres secteurs d'activité traitent leur patrimoine informationnel et font la gestion de ses RI, comme le commerce de détail, secteur automobile, télécoms, industrie, etc. et de chercher si le degré de maturité de leur traitement change selon le domaine.

Du côté méthodologie, le mieux aurait été de proposer des questionnaires entièrement anonymisés pour obtenir un niveau de biais de désirabilité plus bas. Il s'agit d'un sujet sensible et stratégique qui peut dévoiler les faiblesses (et forces) d'une entreprise. Il n'est pas exclu que certaines questions n'aient reçu que des réponses partielles. La collecte des données ne s'est pas déroulée comme nous l'avions prévue (cf. 3.3.2) et cela semble avoir limité notre recherche. En outre, l'accès à l'organigramme et l'utilisation libre des données auraient été utiles pour obtenir des réponses plus exploitables.

Nous constatons aussi un manque d'ouvrages spécialisés sur la législation touchant l'information en Suisse. La rédaction d'un guide permettrait de rassembler des informations très dispersées à ce sujet et pourrait être utile aux managers de risque et aux organisations en générale.

Finalement, nous concluons qu'il reste beaucoup à étudier sur la meilleure façon de tirer profit des actifs informationnels et des informations d'une entreprise. L'entreprise doit structurer sa gestion de l'information, pouvoir disposer de l'information et la mettre à disposition au moment opportun et comme disait Harbulot (2005) « apprendre à détecter le risque informationnel et ne pas se laisser déstabiliser par l'information ». Nous avons trouvé que certains articles traitant des RI datent du début des années 2000 et restent toujours d'actualité (par exemple Lemieux 2004a,b pour ce qui concerne la gestion des RI en entreprises). D'un autre côté, nous avons remarqué une importance grandissante des études sur la gestion des risques, en intelligence économique et des disciplines touchant la Gouvernance de l'information avec des perspectives plus pratiques. La méthode adoptée par Desjardins (2011), par exemple, laisse présager qu'une évolution est en cours, même si elle semble s'imposer lentement.

Bibliographie

AFF, ADMINISTRATION FEDERALE DES FINANCES, 2015. Manuel de gestion des risques de la Confédération. *efv.admin.ch* [en ligne]. 10 septembre 2015. [Consulté le 29 mars 2017]. Disponible à l'adresse : https://www.efv.admin.ch/efv/fr/home/themen/finanzpolitik_grundlagen/risiko_versicherungspolitik.html

ARMA International, 2009. *Evaluating and mitigating records and information risks : an ARMA International guideline.* Overland Park, Kansas : ARMA International. ISBN 978-1931786850

ASSEMAN, Audrey et DUPONT, Benoit, 2011. Le vol interne d'informations : modéliser et mesurer les facteurs de risque. *Sécurité et stratégie* [en ligne] 2011/1 (5), p. 5-16. DOI : 10.3917/sestr.005.0005. [Consulté le 3 avril 2017]. Disponible à l'adresse : https://www.cairn.info/revue-securite-et-strategie-2011-1-page-5.htm

BANAT-BERGER, Françoise, DUPLOUY, Laurent et HUC, Claude, 2009. *L'archivage numérique à long terme : les débuts de la maturité ?* Paris : Documentation Française. ISBN 978-2-11-006942-9

BELOUEZZANE, Sarah, 2014. Orange de nouveau victime d'une cyberattaque massive. *Le Monde : Economie* [en ligne]. 07 mai 2014. [Consulté le 05 janvier 2018]. Disponible à l'adresse : http://www.lemonde.fr/economie/article/2014/05/07/orange-de-nouveau-victime-d-une-cyberattaque-massive_4412779_3234.html

BOUZON, Arlette, 2001. Risque et communication dans les organisations contemporaines. *Communication et organisation* [en ligne]. N° 20, décembre 2001. DOI : 10.4000/communicationorganisation.2548. [Consulté le 3 avril 2017]. Disponible à l'adresse : https://communicationorganisation.revues.org/2548

BOY, Louis, 2014. Les révélations embarrassantes du piratage de Sony Pictures. *France Info : Culture* [en ligne] 04 décembre 2014. [Consulté le 05 janvier 2018]. Disponible à l'adresse : Disponible à l'adresse : https://www.francetvinfo.fr/culture/cinema/les-trois-revelations-embarrassantes-du-hack-de-sony-pictures_764337.html

CAPRIOLI, Eric et al.,2007. *Protection du patrimoine informationnel* [en ligne]. Paris : FedISA, CIGREF. [Consulté le 30 juillet 2017]. Disponible à l'adresse : https://cigref.typepad.fr/cigref_publications/RapportsContainer/Parus2007/Protection_patrimoine_informationnel_CIGREF_FEDISA_2007_web.pdf

CLUSIF (Club de la sécurité de l'information français), 2009. La gestion des risques. Concepts et méthodes. *Clusif* [en ligne]. Révision 1 du 28 janvier 2009. [Consulté le 3 avril 2017]. Disponible à l'adresse : http://ddata.over-blog.com/xxxyyy/0/32/13/25/Risques/CLUSIF-Gestion-des-risques-2008.pdf

COSO. *Wikipédia : l'encyclopédie libre* [en ligne]. Dernière modification de la page le 19 avril 2017 à 11 :17. [Consulté le 09 janvier 2018]. Disponible à l'adresse : http://fr.wikipedia.org/w/index.php?title=COSO&oldid=136593869

DARSA, Jean-David, 2013. *La gestion des risques en entreprise*. Le Mans : Gereso, 2013. ISBN 978-2-35953-198-5

DEFR, DEPARTEMENT FEDERAL DE L'ECONOMIE, DE LA FORMATION ET DE LA RECHERCHE, 2017. La gestion des risques stratégiques et opérationnels. *Portail PME pour petites et moyennes entreprises. Le portail du gouvernement suisse* [en ligne]. Mis à jour le 3

février 2017. [Consulté le 29 mars 2017]. Disponible à l'adresse : https://www.kmu.admin.ch/kmu/fr/home/savoir-pratique/finances/gestion-risques.html

DESJARDINS, 2011. *La gestion des risques informationnels. L'approche adoptée par Desjardins.* Conférence RSI 28 mars 2011 [en ligne]. [Consulté le 3 avril 2017]. Disponible à l'adresse https://www.yumpu.com/fr/document/view/16547444/la-gestion-des-risques-informationnels-colloque-rsi

DELEPORTE, Bénédicte et SFEZ, Betty, 2013. La protection du patrimoine informationnel de l'entreprise : un tour d'horizon (fr). *La Grande Bibliothèque du Droit* [en ligne]. 3 octobre 2013. [Consulté le 20 avril 2017]. Disponible à l'adresse : http://www.lagbd.org/index.php/La_protection_du_patrimoine_informationnel_de_l%E2%80%99entreprise_:_un_tour_d%E2%80%99horizon_(fr)

DIETE, Edwin, 2003. Recordkeeping integrity : assessing records' content after Enron. *The information management journal.* May/June 2003. Vol. 37, issue 3, pp.43-51. ISSN 1535-2897

DESROCHES, Chantal, 2013. *La gestion des risques informationnels dans l'entreprise privée : perspective des gestionnaires de la sécurité* [en ligne]. Montréal : Université de Montréal. Mémoire [Consulté le 2 avril 2017]. Disponible à l'adresse : https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/11469/Desroches_Chantal_2013_memoire.pdf?sequence=6&isAllowed=y

D.N., 2014. Les banques investissent dans le management du risque humain. Le Temps : TMagazine [en ligne] 5 juin 2014. [Consulté le 3 avril 2017]. Disponible à l'adresse : https://www.letemps.ch/economie/2014/06/05/banques-investissent-management-risque-humain

DU MANOIR DE JUAYE, Thibault, 2014. Le risque informationnel au filtre du droit.

Documentaliste-Sciences de l'Information [en ligne] 2014/3 (Vol. 51), p. 37-40. [Consulté le 2 avril 2017]. Disponible à l'adresse : https://www.cairn.info/revue-documentaliste-sciences-de-l-information-2014-3-page-37.htm

ECOLE EUROPEENNE D'INTELLIGENCE ECONOMIQUE, 2011. *Introduction à l'intelligence économique et à la protection du patrimoine informationnel*. [Consulté le 2 avril 2017]. Disponible à l'adresse : http://chaire-sirius.eu/wp-content/uploads/2015/07/2011_intro_a_l_intelligence_eco_eeie.pdf

EDUSCOL, 2015. *Sécurité des systèmes d'information : de la gestion des risques à la confiance numérique* [en ligne]. 3 avril 2015. [Consulté le 29 mars 2017]. Disponible à l'adresse : http://eduscol.education.fr/ecogest/si/SSI/risk_conf

FARINE, Mathilde *et al.,* 2015. Comment les entreprises utilisent nos données. *Le Temps : TMagazine* [en ligne]. 28 décembre 2015. [Consulté le 3 avril 2017]. Disponible à l'adresse : https://www.letemps.ch/economie/2015/12/28/entreprises-utilisent-nos-donnees

FORTIN, Marie-Fabienne et GAGNON, Johanne, 2016. *Fondements et étapes du processus de recherche : Méthodes quantitatives et qualitatives*. Montréal, 2016. ISBN 978-2-7650-5006-3

GAGNON-ARGUIN, Louise et VIEN, Hélène, 1998. *Typologie des documents des organisations. De la création à la conservation.* Québec, Presse de l'Université du Québec.

GHERNAOUTI-HÉLIE Solange, 2007. Risque informationnel : une simple évolution ? *Bulletin HEC* [en ligne]. 16 mai 2007. N° 73, p.34-35. [Consulté le 3 avril 2017]. Disponible à l'adresse : http://www.scarg.org/wp-content/uploads/2013/10/73_Solange.pdf

GOUBET, Fabien, 2016. La protection des données de santé est un numéro d'équilibriste. *Le Temps : TMagazine* [en ligne]. 31 octobre 2016. [Consulté le 3 avril 2017]. Disponible à l'adresse : https://www.letemps.ch/sciences/2016/10/31/protection-donnees-sante-un-numero-dequilibriste

HAGMANN, Jürg, BURGWINKEL, Daniel et WILDHABER, Bruno, 2016. Information Governance. In : I*nformation Governance : A Practical Guide* [livre électronique]. Zurich : KRM. Chapitre 2.4.3 [Consulté le 10 avril 2017]. Disponible à l'adresse : https://www.amazon.de/Information-Governance-Practical-control-information-ebook/dp/B01LJHQRLS/ref=sr_1_6?ie=UTF8&qid=1472997252&sr=8-6&keywords=wildhaber

HAPSIS, 2009. *Le livre bleu : Développer la culture des risques informatiques et informationnels.* Tome VI. [en ligne] Octobre 2009. [Consulté le 3 avril 2017]. Disponible à l'adresse : http://arpagian.eu/wp-content/uploads/2015/09/2009-octobre-Assises-Europ%C3%A9ennes-de-la-S%C3%A9curit%C3%A9-Point-de-vue-de-Nicolas-Arpagian.pdf

HARBULOT, Chistian, 2005**.** La manipulation de l'information, 2005. *Actes du SSTIC* [en ligne] [Consulté le 10 juillet 2017]. Disponible à l'adresse : http://piloupilou.sstic.org/SSTIC05/Entreprise_face_au_risque_informationnel/SSTIC05-Harbulot-Entreprise_face_au_risque_informationnel.pdf

HARLOW Kate, 2012. Managing medical record risks. *Management in practice* [en ligne] 29.3.2012. [Consulté le 3 avril 2017]. Disponible à l'adresse : http://www.managementinpractice.com/featured-articles/managing-medical-record-risks

HASSID, Olivier, 2008. *La gestion des risques*. 2e éd. Paris : Dunod, 2008. Les topos+. ISBN 978-2-10-053661-0

HUYGHE, François-Bernard, [s.d.] Risque informationnel : nouvelle donne. *Huyhe.fr* [en ligne]. [Consulté le 25 juillet 2017]. Disponible à l'adresse : http://www.huyghe.fr/conference_5.htmHuyghe

KERMISCH, Céline, 2012. Vers une définition multidimensionnelle du risque. *VertigO - la revue électronique en sciences de l'environnement [en ligne]. Vol. 12, no. 2.* [Consulté le 25 avril 2017]. DOI : 10.4000/vertigo.12214. Disponible à l'adresse : http://journals.openedition.org/vertigo/12214

KNOWCKERS, 2017. Les risques informationnels de la conformité bancaire. *Knockers* [en ligne]. 28 mars 2017. [Consulté le 3 avril 2017]. Disponible à l'adresse : http://www.knowckers.org/2017/03/les-risques-informationnels-de-la-conformite-bancaire/

LACROIX, Jérémie, 2007. *Analyse et gestion des risques dans les grandes entreprises.Impacts et rôle pour la DSI.* Paris : CIGREF et IERSE, 2007 [en ligne]. [Consulté le 3 avril 2017]. Disponible à l'adresse : http://cigref.typepad.fr/cigref_publications/RapportsContainer/Parus2007/gestion_des_risques/Analyse_et_gestion_des_risques_dans_les_grandes_entreprises_-_impacts_pour_la_DSI-rapport_2007_web.pdf

LÉGER, Marc-André, 2013. *Introduction à la gestion de risque informationnel* [en ligne]. Centre de recherche Hochelaga-Maisonneuve, Montréal, Québec. 1 mars 2013. ISBN 978-2-9813728-1-9. [Consulté le 2 avril 2017]. Disponible à l'adresse : http://www.leger.ca/wp-content/uploads/2015/09/Introduction-%C3%A0-la-gestion-de-risque.pdf

LÉGER, Marc-André, 2015a. Pour une définition du risque informationnel. *Leger.ca* [en ligne]. 2 octobre 2015. [Consulté le 11 avril 2017]. Disponible à l'adresse :

http://www.leger.ca/2015/10/02/pour-une-definition-du-risque-informationnel/

LÉGER, Marc-André, 2015b. Typologie des risques informationnels. *Leger.ca* [en ligne]. 23 octobre 2015. [Consulté le 11 avril 2017]. Disponible à l'adresse : http://www.leger.ca/2015/10/23/typologie-des-risques-informationnels/

LÉGER, Marc-André, 2017. Intro au risque informationnel [enregistrement vidéo]. *YouTube* [en ligne]. 19 février 2017. [Consulté le 29 mars 2017]. Disponible à l'adresse : https://www.youtube.com/watch?v=7f5BnWuCZ68

LEMIEUX, Victoria L.,2004a. *Managing Risks for Records and Information.* Lenexa : Arma International, 2004. ISBN 1-931786-18-6

LEMIEUX, Victoria L.,2004b. Two approaches to Managing Information Risks. *Information Management* [en ligne]. Septembre/Octobre. 2004.Vol. 38, no. 5, pp.56-62. [Consulté le 9 janvier 2018]. Disponible à l'adresse : https://pdfs.semanticscholar.org/21b9/c26d5e9c7806b107504a70fd2461c2c022e8.pdf

LEMIEUX Victoria L. et KRUMWIED Ember D., 2011. Managing records risks in global financial institutions. In : *Managing records in global financial markets, ensuring compliance and mitigating risk.* London, Facet Publishing. p. 91-105. ISBN 978-1-85604-663-3

LESCA, Elisabeth et LESCA Humbert, 2010. *Gestion de l'information.* 2e éd. Cormelles-le-Royal : EMS Editions. ISBN 978-2-84769-130-6

MARBAIX, Jean-Pierre, 2016. Comment identifier vos risques ? *Audipog, jeudi 8 décembre 2016* [en ligne]. [Consulté le 3 avril 2017]. Disponible à l'adresse : http://www.audipog.net/pdf/seminaires/seminaire_2016_3/pres02.pdf

MARESCHAL, Gilbert de, 2003. *La cartographie des risques*. A Savoir 61. Saint-Denis La Plaine : AFNOR, 2003. ISBN 2-12-505071-4

MAYER Nicolas et HUMBERT Jean-Philippe, 2006. La gestion des risques pour les systèmes d'information. *MISC* n°24 [en ligne]. Avril-mai 2006 [Consulté le 29 mars 2017]. Disponible à l'adresse : http://www.nmayer.eu/publis/NMA-JPH_MISC24.pdf

MOINET, Nicolas, 2014. Les risques informationnels, d'une vision statique à une conception dynamique. *Documentaliste-Sciences de l'Information* [en ligne]. 25 septembre 2014. Vol. 51, n° 3, pp. 44-46. . [Consulté le 29 mars 2017]. Disponible à l'adresse : https://www.cairn.info/revue-documentaliste-sciences-de-l-information-2014-3-page-44.htm

MoReq. *Wikipédia : l'encyclopédie libre* [en ligne]. Dernière modification de la page le 06 août 2017 à 01 :53. [Consulté le 09 janvier 2018]. Disponible à l'adresse : http://fr.wikipedia.org/w/index.php?title=MoReq&oldid=139529800

OBSERVATOIRE DE LA GOUVERNANCE DE L'INFORMATION et 3ORG CONSEIL, 2012. *Gouvernance de l'information* [en ligne].[Consulté le 7 avril 2017]. Disponible à l'adresse : http ://www.gouvinfo.org/IAI/wp-content/uploads/Livre-blanc-sur-la-gouvernance-de-linformation-observatoire-GouvInfo-2012-V9.pdf

ORGANISATION INTERNATIONALE DE NORMALISATION, 2009. *Management du risque : principes et lignes directrices* [en ligne] Genève. ISO 31000:2009 [en ligne].[Consulté le 05 janvier 2018]. Disponible sur abonnement à l'adresse : https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:fr

ORGANISATION INTERNATIONALE DE NORMALISATION, 2011.*Technologies de l'information — Techniques de sécurité —Gestion des risques liés à la sécurité de l'information*

[en ligne]. 2e éd. 1 juin 2011. Genève. ISO/CEI 27005:2011(F) [Consulté le 29 juin 2017]. Disponible sur abonnement à l'adresse : http://hesge.snvhosting.ch/documents/1959586/1959586.PDF?filePath=documents%2F&dataPath=data%2F&language=de&runtime=BROWSER

PERREIN, Jean-Pascal, 2012. Le risque informationnel, une menace ou une opportunité. *GouvInfo IAI* [en ligne]. 2 mai 2012 . [Consulté le 10 avril 2017]. Disponible à l'adresse : http://www.gouvinfo.org/IAI/le-risque-informationnel-une-menace-ou-une-opportunite/

PIERANDREI, Laurent, 2015. *Risk management. Gestion des risques en entreprise, banque et assurance.* Paris : Dunod, 2015. ISBN 978-2-10-072256-3

PROTIVITI, 2011. Baromètre du Risk Management 2011, 7e éd. *TNS* [en ligne]. 2011 [Consulté le 4 avril 2017]. Disponible à l'adresse : https://www.tns-sofres.com/publications/barometre-du-risk-management-2011

ROUAUD, Pauline et BARRIOL, François, 2012. *Etude sur les risques et opportunités liés à l'e-réputation des entreprises.* [en ligne] Paris : Cigref. [Consulté le 3 avril 2017]. Disponible à l'adresse : https://www.cigref.fr/wp/wp-content/uploads/2012/04/2012_E-reputation_Etude_des_risques_et_opportunites_lies_a_-l_e-reputation_des_entreprises_CIGREF.pdf

ROUHIER, Stéphane, 2008. *Protection de l'information : enjeux, gouvernance et bonnes pratiques* [en ligne]. Paris : Cigref. [Consulté le 3 avril 2017]. Disponible à l'adresse : https://www.cigref.fr/cigref_publications/RapportsContainer/Parus2008/Protection_information_2008.pdf

SMALLWOOD, Robert F., 2014. *Information Governance : Concepts, Strategies, and Best Practices.* Hoboken : Wiley. ISBN 978-1-118-21830-3

SOCIÉTÉ GÉNÉRALE, 2017. La gestion des risques bancaires. *Société Générale* [en ligne].[Consulté le 3 avril 2017]. Disponible à l'adresse : https://www.societegenerale.com/fr/comprendre-la-banque/le-metier-de-banquier/la-gestion-des-risques-bancaires

UNIRIS (Services de ressources informationnelles et archives), 2016. *Records management et gouvernance informationnelle : Concepts et explications.* [en ligne] Université de Lausanne.11 juin 2014. Mise à jour 28 janvier 2016. [Consulté le 3 avril 2017]. Disponible à l'adresse : : https://www.unil.ch/uniris/files/live/sites/uniris/files/documents/references/UNIL_RM_Gouvernance_Info_concepts_explications_VF-1.pdf

VALLÈS, Lyonel, 2015. Le risque informationnel et l'urgence de le gérer de façon adéquate. *Lyonel Vallès, CISA, CRISC* [en ligne]. 20 décembre 2015.[Consulté le 3 avril 2017]. Disponible à l'adresse : http://lyonelvalles.com/2015/12/20/le-risque-informationnel-et-lurgence-de-le-gerer-de-facon-adequate/

VERMEYS, Nicolas W., 2009. *Qualification et quantification de l'obligation de sécurité informationnelle dans la détermination de la faute civile* [en ligne]. Université de Montréal. Thèse. [Consulté le 29 mars 2017]. Disponible à l'adresse : https://papyrus.bib.umontreal.ca/xmlui/handle/1866/3663

VIGOUROUX-ZUGASTI Eloria, 2015. L'importance de l'évaluation de l'information. *Ricsa* [en ligne]. 15 février 2015. [Consulté le 3 avril 2017]. Disponible à l'adresse : https://ricsa.hypotheses.org/64

Annexe 1 : Exemple de fiche de risque

Plan de mesures				
Risque n° et nom	*1*	*Changements technologiques pouvant mettre l'entreprise en péril.*		
Responsable du risque	*Hans Mustermann, responsable Technologie*			
Catégorie du risque	*externe*	*stratégique*	*opérationnel*	*financier*
Description du risque	*Différentes technologies pouvant mettre en danger le modèle commercial de l'entreprise ont été lancées sur le marché. Si les concurrents introduisent de nouveaux produits sur le marché plus rapidement que Muster SA, les répercussions peuvent être lourdes de conséquences.*			
Facteurs/causes du risque	· *Introduction de nouveaux produits sur le marché reportée* · *Investissements insuffisants en R&D* · *Mauvaise stratégie dans l'établissement du portefeuille de produits*			
Stratégie du risque	*accepter*	*réduire*	*éviter*	*transférer*
	·Adaptation agressive des stratégies et des mesures afin de constituer un portefeuille à haut rendement *· Leader du marché dans le développement de produits de substitution et analyse des opportunités*			
Mesures existantes	*· Augmentation du budget R&D de 250% au dernier exercice* *Entrée en vigueur de nouvelles directives afin de recruter des collaborateurs compétents dans le domaine R&D*			
Plan de mesures	***Responsable***	***Etape majeure***	***Date***	***Statut***
1. Préparation des prototypes pour la commercialisation	*Hans Muster*	*Prototype 1* *Prototype 2*	*30.9.2009* *31.12.2009*	*ouvert* *ouvert*
2. Acquisition d'un fournisseur remplaçant	*Fritz Muster*	*Offre d'acquisition*	*30.6.2009*	*initié*
3. Recrutement de deux nouveaux collaborateurs en R&D	*Anna Muster*	*Embauche collaborateur 1* *Embauche collaborateur 2*	*30.6.2009* *31.7.2009*	*terminé* *terminé*

(DFER, 2017)

Annexe 2 : Principales normes et référentiels concernant la sécurité de l'information

ISO 11799:2015 - « Information et documentation - Exigences pour le stockage des documents d'archives et de bibliothèques »

ISO 13335 - Normes qui donnent des lignes directrices pour la gestion de la sécurité. « C'est un guide de management de la sécurité des systèmes d'information qui trouve son origine dans des rapports techniques (...) considérés comme des références pour toutes personnes s'intéressant aux systèmes d'information. » (Lacroix 2007, p.50) La norme se décompose en cinq parties.

ISO 15489 - Norme internationale pour le Records management, elle en identifie les éléments et fournit un cadre et un aperçu de haut niveau des principes fondamentaux de RM. La deuxième partie de la norme, ISO 15489-2:2001, contient les spécifications techniques et une méthodologie pour sa mise en œuvre. (Smallwood 2014, p.79)

ISO 16175-1/2/3:2010 - « Principles and Functional Requirements for Records in Electronic Office Environments »

ISO 17799 - « Code de pratique pour la gestion de sécurité d'information ». Norme internationale publiée en décembre 2000, avec 2e édition en 2005. Cette norme a pour origine la première partie du British Standard BS 7799. (Lacroix 2007, p.49). Il s'agit d'un ensemble de bonnes pratiques destinées à être utilisées par tous ceux qui sont responsables de la sécurité de l'information et des systèmes d'information (Lacroix 2007, p.49).

ISO 18128 - « Information et documentation - Evaluation du risque pour les processus et systèmes d'enregistrement, » Pour la gestion des documents d'activité de l'institution, aussi utile pour des auditeurs et pour les gestionnaires du risque.

ISO 27001 - « Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information – Exigences ». Fondée sur une approche de gestion du risque. Traite de la gestion de la sécurité de l'information, décrit comment mettre en place un Système de Gestion de la Sécurité de l'Information (SGSI) qui permet de choisir les mesures appropriées afin de protéger les actifs de l'entreprise. (Lacroix 2007, p.50) Cette méthode d'audit est d'origine anglaise, anciennement BS7799. Il s'agit de la plus utilisée au monde aujourd'hui (Caprioli 2007, p.7). L'ISO 27001 est une approche basée sur les processus qui définit l'ensemble des tests et contrôles à effectuer pour s'assurer du bon respect d'ISO 17799. (Lacroix 2007, p.50). Pour Smallwood (2014), elle serait même identique à la norme ISO 17799.

ISO /CEI 27002 - « Code de bonne pratique pour la gestion de la sécurité de l'information, qui décrit les mesures de sécurité de l'information » (Léger 2013, p.131)

ISO/CEI 27005 - Nous semble la principale à citer dans le cadre de ce travail parce qu'elle traite spécifiquement de gestion des risques en sécurité de l'information. Publiée en 2008, révisée en 2011, cette norme n'a pas de mécanismes de certification, elle fournit des lignes directrices relatives à la gestion des risques informationnels et vient en appui aux concepts généraux énoncés dans l'ISO 27001 et autres normes de la famille 27000 (Léger 2013, p.130). Il est important de connaître les terminologies de l'ISO 27001 et ISO 27002 pour bien la

comprendre. Cette norme a été conçue pour aider à la mise en place de la sécurité de l'information basée sur une approche formelle de gestion des risques et est applicable à tous les types d'organisations (Léger 2013, p.131). Léger ne la considère pas comme une méthodologie pour la gestion de risque, « elle donne un cadre normatif qui pourra être utilisé pour l'élaboration ou la validation de méthodologies de gestion de risque informationnel (...) [mais] Il appartient à l'organisation de définir son approche. » (Léger 2013, p.131) Dans sa deuxième édition, le cadre a été mis à jour pour tenir compte du contenu des documents de gestion des risques de l'ISO 31000:2009, ISO/CEI 31010:2009 et Guide ISO 73:2009 Management du risque - Vocabulaire. Elle prétend aussi aider les utilisateurs à la mise en œuvre de l'ISO 27001 (Gasiorowski-Denis, 2011).

ISO 30300 Series - Porte sur la création et gestion des Records en accord avec les stratégies organisationnelles (Smallwood 2014, p.81)

ISO 31000 - « Management du risque - Principes et lignes directrices ». C'est une norme de gestion des risques au sens large qui indique les « principes et lignes directrices génériques » de gestion des risques, applicable à un large éventail d'activités organisationnelles. (Smallwood 2014, p.77)

ISO/CEI 38500 - Norme internationale qui fournit des principes et des conseils de haut niveau pour les cadres supérieurs et les directeurs en vue d'une utilisation efficace et efficiente de l'informatique (Smallwood 2014, p.79)

Bâle I et Bâle II – ensemble de recommandations et normes pour mieux appréhender les risques bancaires

COSO - « Référentiel de contrôle interne défini par le Committee Of Sponsoring Organizations of the Treadway Commission. Il est utilisé notamment dans le cadre de la mise en place des dispositions relevant des lois Sarbanes-Oxley, SOX ou Loi de sécurité financière, LSF, pour les entreprises assujetties respectivement aux lois américaines ou françaises (...) [il est] destiné à fournir une assurance raisonnable quant à la réalisation des trois objectifs suivants : l'efficacité et l'efficience des opérations ; la fiabilité des informations financières ; la conformité aux lois et règlements.» (Wikipédia)

MOREQ (Model Requirements for the Management of Electronic Documents and Records, puis Modular Requirements for Records Systems) « Recueil d'exigences pour l'organisation de l'archivage, élaboré dans le cadre de l'Union européenne. C'est une approche opérationnelle de la norme de gestion des documents d'archives ISO 15489. » Il s'agit d'un ensemble de recommandations pour le records management appliqué aux archives électroniques. (Wikipédia)

Il existe beaucoup d'autres normes qui touchent l'information mais nous ne les aborderons pas, car il faut délimiter le travail. Nous pouvons en mentionner quelques-unes à titre d'exemple :

Normes IAS/IFRS - pour la comptabilisation du capital immatériel de l'organisation

SOX (Sarbanes Oxley) – loi des Etats-Unis imposant de nouvelles règles sur la comptabilité et la transparence financière

Solvabilité II - concerne la qualité des données touchant les compagnies d'assurance

Annexe 3 : Liste non-exhaustive de méthodes et outils

COBIT (Control objectives for information & related technology) - « Le référentiel COBIT est une méthode de Maîtrise des Systèmes d'Information et d'audit éditée par l'ISACA (Information System Audit & Control Association) en 1996. C'est un cadre de contrôle qui vise le pilotage des risques liés aux Systèmes d'Information. Ce référentiel utilisable aussi bien par les managers que les utilisateurs permet de faire des liens entre les risques métiers, les mesures de contrôle et les questions techniques relatives aux SI. » (Lacroix 2007, p.54)

EBIOS (Expression des Besoins et Identifications des Objectifs de Sécurité) - Méthode développée en 1995 par la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI) rattachée au SGDN (Secrétariat Général de la Défense Nationale). Cette méthode est un outil de gestion des risques liés à la sécurité des systèmes d'information, de communication sur les risques liés aux systèmes d'information, d'arbitrage qui permet de justifier la prise de décisions. (Lacroix 2007)

FEROS - Comme EBIOS, « méthode particulièrement adaptée pour bâtir une cible de sécurité pour un produit sensible du type cible de sécurité d'un FIREWALL ou du masque de la carte bancaire, par exemple. » (Caprioli 2007, p.6)

Generally Accepted Recordkeeping Principles Maturity Model® (GAR Principles) - Publié en 2009 par ARMA International, Les Principes sont un modèle de maturité en Gouvernance de l'Information utilisé comme évaluation préliminaire des programmes et des pratiques de tenue de dossiers (Smallwood 2014, p.29). Il peut être utilisé pour élaborer une évaluation de l'état actuel des pratiques de tenue des documents d'une organisation, identifier les lacunes, évaluer les risques et élaborer des priorités pour les améliorations souhaitées (Smallwood 2014, p.34).

MARION (Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux) - Conçue par le CLUSIF (Club de la Sécurité de l'Information Français), cette méthode n'est plus mise à jour depuis 1998. Le CLUSIF propose désormais la méthode MEHARI (Méthode d'harmonisation et d'analyse des risques). (Lacroix 2007 p. 53) Cette norme « présente toujours un grand intérêt didactique car les questions sont regroupées dans 27 facteurs qui traitent l'ensemble des questions de sécurité informatique et télécoms sur un axe déterminé ». (Caprioli 2007, p.6)

MEHARI (Méthode harmonisée d'analyse des risques) - « Méthode créée par le CLUSIF (Club de la Sécurité de l'Information Français) dans le but d'aider les Responsables de la Sécurité de Système d'Information dans leurs attributions managériales. Bien que développée pour ce type de fonction spécifique, cette méthode peut aussi être utilisée par les toutes les fonctions qui traitent de problématiques similaires (risk managers, etc.) (...) Un des avantages de cette méthode réside dans le fait qu'elle est compatible avec les principales normes ISO sur la sécurité des systèmes d'information, à savoir les normes ISO 13335, 17799, 27001 ». (Lacroix 2007, p.51) « Méthode intéressante mais inductive. Comme un mécano, cela dépend de la construction du questionnaire qui en est faite ». (Caprioli 2007, p.6)

Outils de sécurité physique - Broyeurs, armoires à clés, moyens de contrôle d'accès aux bâtiments, etc. (Rouhier 2008, p.26)

RiskIT - Référentiel portant sur les risques IT, édité par l'AFAI (Eduscol 2015, p.3)

ValIT - Référentiel basé sur CobiT et complémentaire à celui-ci. Explique comment une entreprise peut tirer la meilleure valeur possible de ses investissements informatiques (Eduscol 2015, p.3).

Autres outils :

Bug Track de Symantec – système de suivi des bugs/bogues logiciels ou défauts, BDD sur vulnérabilités

Cartographie des risques - document qui recense et synthétise les risques

Continuity Plan - progiciel pour mettre en place un plan de continuité, éviter la perte de disponibilité, accessibilité de l'information

CRAMM – méthode d'analyse et de maîtrise des risques concernant le SI d'une entreprise, conforme aux normes BS7799 et ISO 177999

CVE, Common Vulnerabilities and Exposures - dictionnaire d'informations publiques relatives aux vulnérabilités de sécurité, géré par le MITRE, soutenu par le Département de la Sécurité intérieure des Etats-Unis.

CWE (Common Weakness Enumeration) du MITRE – BDD, liste des vulnérabilités que l'on peut rencontrer dans les logiciels. Elle est maintenue par l'organisme américain MITRE

Cyber Risk Deep Dive – études, analyses, formations ou solutions matérielles et logicielles pour se protéger ou contrecarrer et minimiser l'impact des cyberattaques

IAM (Identify and access management) software – solutions de gestion des identités et des accès

IGRM (Information Governance Reference Model) – modèle de référence de la gouvernance de l'information de l'entreprise créé par EDRM

ITIL (Information Technology Infrastructure Library) – ensemble d'ouvrages recensant les bonnes pratiques du management du système d'information.

Nessus – outil de sécurité informatique, logiciel NVA (Network Vulnerability Analyzer) le plus connu

NVAS - logiciel d'identification de vulnérabilités technologiques

OCTAVE - suite d'outils, techniques et méthodes créées pour l'évaluation des risques basée sur la sécurité de l'information stratégique et la planification

Security Focus - site web anglophone de référence, consacré à la sécurité informatique. Il héberge un système de suivi de bugs et des vulnérabilité, BDD sur vulnérabilités

Outils de gestion de l'information : systèmes d'identification/authentification (login et password; identifiant et OTP; certificat électronique sur carte à puce ou clé USB; clé Confidential Defense; carte à puce avec identifiant et mot de passe; solutions biométriques; RFID)

VPN (Virtual Private Network) – un réseau privé virtuel est un système permettant de créer un lien direct entre des ordinateurs distants, en isolant ce trafic.

Annexe 4 : Grille de lecture

	Littérature professionnelle (normes, standards, associations, consultants)	Littérature académique, recherche scientifique	Lois, directives, réglementations
1) Définition risque			
2) Définition risque informationnel			
3) Identification des risques, types de risques informationnels			
4) Evaluation des risques informationnels			
5) Traitement, mitigation des risques informationnels			
6) Normes pour la gestion des risques informationnels			
7) Logiciels, outils pour l'analyse des risques informationnels			
8) Rôles et responsabilités			

Annexe 5 : Demande d'entretien

Sujet : Participation à une recherche sur les risques informationnels dans les organisations

Madame, Monsieur,

Dans le cadre de nos études en sciences de l'information à la HEG, nous réalisons un travail sur les risques informationnels dans les domaines bancaires, médicaux, scientifiques, juridiques et dans les organisations internationales.

Comme vous êtes responsable des archives ou de la documentation au sein de ……., notre professeure Madame Basma Makhlouf Shabou nous a recommandé de solliciter votre participation à cette recherche. Nous vous serions reconnaissantes de bien vouloir nous accorder 45 minutes durant lesquelles nous discuterons des risques informationnels dans votre organisation.

Pour ce faire, nous vous proposons les dates de rencontres suivantes : …… Les questions vous seront envoyées au préalable. L'entretien sera enregistré et transcrit. Cette transcription vous sera envoyée pour vérification si vous le souhaitez.

Nous vous remercions d'avance de votre participation et contribution à cette étude. Dans l'attente de vos nouvelles, nous vous présentons, Madame/Monsieur, nos meilleures salutations.

Giselle Castelo et Monika Bolliger

Annexe 6 : Formulaire de consentement pour enregistrement de l'entretien et libre accès des données

Titre du projet : **Risques informationnels dans les organisations : état de l'art des typologies, méthodes, techniques et outils de gestion**

Responsables du projet (personne à contacter pour informations) : Giselle Castelo (email) et Monika Bolliger (email)

Ecole : HEG, Genève
Master en sciences de l'information
Filière : information documentaire
Bâtiment B, Campus de Batelle,
Rue de la Tambourine 17,
1227 Carouge

Directrice de recherche :Prof : Madame Basma Makhlouf-Shabou

Objectifs du projet

L'objectif de ce travail est d'établir un état de l'art des risques informationnels dans les organisations en se basant sur la littérature récente. Nous présentons les différentes approches et les différents outils de la gestion des risques.

Dans un deuxième temps, grâce à votre participation, nous pourrons confronter la littérature analysée à la réalité sur le terrain et votre avis d'experts nous permettra d'enrichir les informations récoltées et de cadrer, donner un sens et une direction à notre étude.

Tâches

Pour cette étude, nous vous soumettons des questions concernant la gestion des risques informationnels dans votre organisation. Nous enregistrons l'entretien, sa durée est de 45 minutes. Nous retranscrirons l'entretien et en ferons l'analyse.

Si l'une d'entre nous souhaite poursuivre et rendre publique cette étude, les données produites seront accessibles (open access), à moins que vous souhaitiez qu'elles demeurent confidentielles.

Consentement du/de la participant-e

J'ai pris connaissance du but de l'étude. J'accepte de participer à cette étude.

□ Oui

□ Non

J'accepte que les informations recueillies soient rendues publiques

□ Oui

□ Non

Nom du participant(e) Signature du participant(e) Date

Annexe 7 : Questionnaire

A- Profil démographique du participant

1- Quel est votre nom, prénom, âge ?

2- Quelle est votre formation ?

3- Quelle est votre fonction, quel est le titre du poste ?

4- Depuis combien de temps travaillez-vous à ce poste ?

5- Quelles sont vos tâches, pouvez-vous les décrire ?

B- Profil organisationnel

1- Environnement : quel est le domaine, le secteur d'activité de votre organisation ?

2- Avez-vous un organigramme ? pouvez-vous nous le fournir ?

3- Quelle est votre mission ?

4- Quelle est la taille de l'organisation ?

5- Qui sont les clients ?

6- Qui sont les partenaires ?

C-Questionnaire risques informationnels

1. Définition du risque

1.1- Comment définissez-vous le risque ou comment le risque est-il défini dans votre organisation ?

2. Définition du risque informationnel

2.1- En quoi consiste le patrimoine informationnel ou les actifs informationnels de votre organisation ?

2.2- Quelles sont les qualités de l'information ?

2.3- Comment définissez-vous le risque informationnel ? Est-ce une définition d'un manuel ?

3. Gestion des risques : Identification, types de risques informationnels

3.1- Quels types de risques sont gérés dans votre organisation ? Est-ce que le risque informationnel en fait partie ?

3.2- Avez-vous une typologie, un classement des risques ? Utilisez-vous un manuel de référence ? Si oui, lequel ?

3.3- Est-ce que vous avez une typologie, un classement des risques informationnels ? Classez-vous les risques dans des catégories ?

3.4- Pourriez-vous citer des risques informationnels ?

3.5- Lesquels sont les plus importants ?

3.6- Est-ce que vous perdez des données ?

4. Gestion des risques : évaluation des risques informationnels

4.1- Comment évaluez-vous ou mesurez-vous les risques informationnels ? Quelle méthode d'évaluation utilisez-vous ? Référence ? Grille ? Pouvons-nous en avoir une copie ? Est-ce que la gestion des risques informationnels diffère de la gestion de risques en général ?

4.2- Décrivez-vous les risques ou des scénarios de risques ?

4.3- Avez-vous créé une fiche, un tableau par risque ?

4.4- Les risques informationnels sont-ils appliqués à l'ensemble de l'entreprise ou uniquement dans un périmètre bien défini (seulement un secteur, une activité, une infrastructure spécifique) ?

4.5- Est-ce qu'il y a une liste de risques spécifiques par région ou pays ? (Organisation internationale)

5.Gestion des risques : traitement, mitigation des risques informationnels

5.1- Comment traitez-vous les risques informationnels ?

5.2- Avez-vous un tableau, un modèle, une marche à suivre pour traiter les risques ?

5.3- Faites-vous recours à des services d'externalisation (informatique, facturation, SI, réseaux ou télécommunication, logistique, transports) ?

5.4- Avez-vous un Disaster Recovery Plan ou plan de secours ?

5.5- Les risques sont-ils contrôlés, suivis ? Comment ? *(monitoring, audit)*

6. Normes et lois pour la gestion des risques informationnels

6.1- Quelles normes suivez-vous ?

6.2- Y-a-t-il des normes spécifiques à votre domaine d'activité ?

6.3- Quelles sont les lois (en général) que vous devez respecter concernant la gestion de la sécurité de l'information dans votre organisation ? Quelle est la législation ?

7. Dispositifs investis (logiciels, outils, tableaux, méthodes, ...) pour l'analyse des risques informationnels

7.1- Avez-vous une politique pour la gestion des risques informationnels ? Si, oui, pouvons-nous en avoir une copie ?

7.2- Comment cette politique est-elle communiquée au sein de l'organisation ?

7.3- Quels outils utilisez-vous pour la gestion des risques informationnels ?

7.4- Quelles méthodes utilisez-vous pour la gestion des risques informationnels ? des méthodes existantes, adaptées à vos besoins, créées par votre organisation ?

7.5- Que faites-vous pour éviter la perte, l'utilisation non-autorisée des documents ?

7.6- Qu'avez-vous comme outils / méthodes pour le délai de conservation des docs ?

8. Rôles et responsabilités

8.1- Y-a-t-il une personne ou une unité en charge de la gestion des risques informationnels. Si oui, quel est son titre ? Pour les grandes entreprises : Y-a-t-il des responsables locaux ou sectoriels ?

8.2- Les collaborateurs sont-ils sensibilisés aux risques liés à leurs activités ? Comment ? Mesurez-vous l'impact de cette sensibilisation ?

9. Question ouverte

9.1- Avez-vous d'autres éléments que vous souhaitez aborder avec nous ?

Annexe 8 : Risques risques informationnels cités dans les entretiens

Risques cités	HOP	DS	IRE	OI	Banque
Indisponibilité d'une information - n'avoir pas la bonne information au bon moment pour assurer prestation - *e-discovery* (disponibilité relative des mails, car il faut du temps pour les retrouver)	x	x			x
Divulgation de données confidentielles, fuites de données confidentielles, mauvais usage ou utilisation illégale des données (atteinte à l'intégrité des données), accès à la boîte mail des collaborateurs	x				x
Accessibilité limitée des locaux, des armoires, des documents	x				
Accessibilité à l'information					x
Détérioration des archives - Corruption des données	x				x
Vol de données, infiltration avec clés usb		x			
Perte ou fuite d'information (général)	x	x	x	x	x
Mauvais classement, mauvaise indexation, pertes ou manques de données, de pièces d'archives au sein d'un fonds, confusion et mélange de noms ou dates, documents non envoyés, non sélectionnés, non identifiés par le service producteur du doc., oublis de dossiers sur les bureaux	x				x
Négligence ou non-maîtrise dans la gestion de fonds, non-archivage de documents à conserver	x	x			x
Management de l'information				x	

Interprétation erronée des informations (par les médias)	x				
Difficulté à suivre, tracer les informations, notamment les données sensibles et les e-mails		x			x
Risques dans la communication, les échanges		x			
Mensonge des gens sur leur identité - non-authenticité des papiers - transmission de fausses informations (papiers jetés)		x			
Transmission d'informations justes au citoyen pour qu'il puisse répondre juste aussi		x			
Garantir la suppression des données, ne pas tout garder, droit à l'oubli, délais de conservation flous, législations incompatibles de différents pays.		x			x
Plutôt risque informatique : écrasement de fichiers, laisser l'ordinateur ouvert, ne pas changer de mot de passe, cyberattaque, non enregistrement dans les ECM ou les serveurs communs,		x		x	
Obsolescence des outils, non- récupération des données, illisibilité des fichiers, des formats		x			x
Gestion de l'information sur support audio, durée de conservation, qualité des enregistrements audio qui peuvent aussi avoir une valeur contractuelle					x
Gestion des e-mails, des données non-structurées et de toute la communication en réseau, e-mails sont stockés (on ne peut les détruire), mais ne sont pas archivés, problème de traçabilité, d'accessibilité, de perte de docs importants, procédures d'*e-discovery*					x

Annexe 9 : Mesures de mitigation citées aux entretiens

Risque	**Mesure de mitigation**	**source**
Fuite d'information	Secret professionnel - le devoir de réserve en tant que fonctionnaire - sermon - paramétrage du système	DS
Mauvais usage ou divulgation de données confidentielles par rapport au dossier patient, notamment au téléphone ou entre collègues	Secret professionnel ; ne pas donner des informations à qui n'a pas le droit ; sensibilisation	HOP
Divulgations ou fuites de données confidentielles administratives ou relatives à la stratégie de l'entreprise	Fournir l'information demandée, la cibler et ne rien fournir de plus ; sensibilisation	HOP
Document mal classé	Utilisation de systèmes de recherche	B
Effraction (locaux)	Fermer à clé, utiliser des badges	HOP
Documents abîmés par l'humidité des locaux	Contrôle hygrométrique	HOP
Documents abîmés par rongeurs	Eviter les rats, souris	HOP
Panne informatique	Anticipation, plans de contingence	HOP
Indisponibilité des locaux, de l'information ou des personnes (ex. épidémie)	BCP/BCM (Business Continuity Plan/Management)	IR

Annexe 10 : Lois mentionnées par les répondants

Loi	B	OI	IRE	HOP	DS
LPD	x		x		
Loi sur la protection des données cantonale				x	x
LAr	x		x		
LArch (niveau cantonal)				x	x
Olico	x				
GDPR	x				
EMIR	x				
MIFID2	x				
CISO (norme Européenne)	x				
FINMA	x				
Associations professionnelles	x				
Convention avec les Archives d'Etat				x	
LSI (Loi sur la Sécurité informatique)			x		
LPers			x		
LTrans			x		
CO			x		
Lois sur les activités métier				Loi cantonale sur la santé	Loi cantonale sur la police, entre autres
Législation du canton			x	x	x

Annexe 11 : Cartographie des Risques informationnels en approche transversale

Cartographie des Risques informationnels en approche transversale

Objectifs de l'information									Services ou départements concernés					Risque No	Titre du risque	Détail, description du risque	Causes	Mesures	Probabilité *	Impact **	Score	Traitement					Responsable du risque
Intègre	Disponible	Confidentielle	Communicable	Partageable	Engageante	Pertinente	Complète	Utile à l'avenir	Direction	Enseignement	Communication	Administration	Gestion des risques						(1à 5)	(1 à 5)	(prob.*imp.)	ignorer	accepter	réduire	éviter	transférer	M. / Mme ..
x	x	x	x					x				x		1	Détérioration, destruction des informations	Mauvaise conservation des archives	Locaux inadaptés, présence de rongeurs	Contrôles hygrométrique, sanitaire et incendie	2	5	10			x			
	x		x	x			x		x	x	x	x	x	2	Indisponibilité d'informations	Indisponibilité d'informations au moment opportun, information incomplète	Mauvais rangement des dossiers, mauvaise entrée des données, problèmes techniques	Sensibilisation, mise en place GED, RM, sécurisation des SI, veille,etc	5	3	15			x			
		x							x	x	x	x	x	3	Divulgation d'informations confidentielles	Divulgation de données personnelles, des données stratégiques	Facteur humain (volontaire ou non), erreur technique	Sensibilisation, prévention, sécurisation des SI	2	4	8			x			
x						x		x	x	x	x	x	x	4	Informations erronées	Données financières erronées, erreur de paramétrage du SI, données des étudiants et du personnel inexactes	Facteur humain (volontaire ou non), erreur technique	Sensibilisation, prévention, paramétrage correct des SI	4	3	12			x			
x			x	x	x	x			x	x	x	x	x	5	Atteinte à l'image, mauvaise qualité des prestations	Indisponibilité des outils pour l'apprentissage	Outils pour l'accès et le partage d'information indisponibles ou pas satisfaisants (PC, réseau, imprimantes, scanner). Ressources limitées dans la bibliothèque (base de données, livres)	Contrôle du bon fontionnement des outils. Investissement dans le fonds de la bibliothèque. Veille réputationnelle active et présence dans les réseaux sociaux.	3	4	12			x			

Niveaux de probabilité			**Niveaux d'impact**	
	Fréquence ou	**pourcentage**		**Financier par ex.**
1 - Improbable	< 5 ans	0-5%	**1 - Insignifiant**	< 5'000.-
2 - Très rare	tous les 5 ans	5-20%	**2 - Réduit/limité**	< 10'000
3 - Rare	annuel	20-40%	**3 - Perceptible**	< 20'000
4- Possible	mensuel	40-70%	**4 - Critique**	< 100'000
5 - Certain	hebdomadaire	70-100%	**5 - Catastrophique**	> 100'000

* Pour une liste avec des menaces types et vulnérabilités avec les méthodes respectives d'appréciation, consulter ISO/CEI 27005 : 2011, annexes C et D.

**Probabilité du risque résiduel selon échelle qualitative ou quantitative. Les risques informationnels peuvent être évalués selon les mêmes échelles que les autres risques de l'entreprise. Nous avons pris l'exemple des critères que nous avions cités en 2.7 pour des raisons de commodité et non parce que nous les privilégions par rapport à d'autres échelles de mesures. La plupart des gestionnaires de risque créent des tableaux annexes pour expliquer leurs critères. Nous en mettons ici à titre d'exemple.

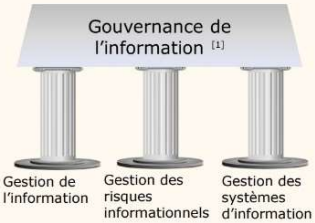
***Certaines organisations prennent en considération l'impact financier, humain, celui sur la réputation ou la prestation, par ex. On peut avoir des échelles qualitatives ou quantitatives, en francs, en pourcentages, etc.

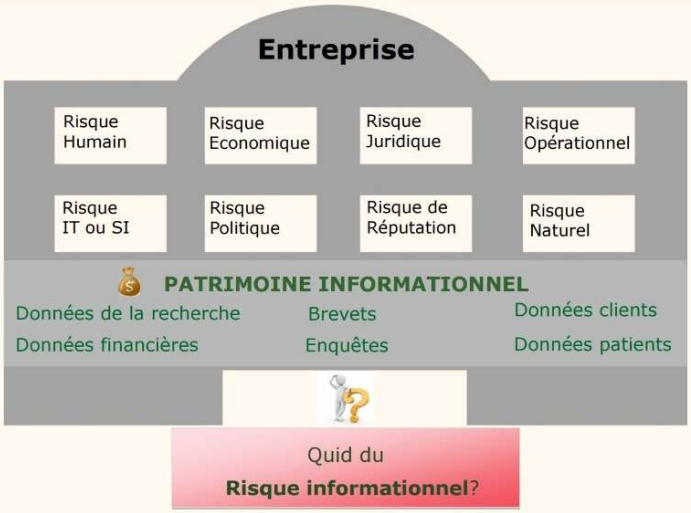
Annexe 12 : Poster

Gestion des Risques Informationnels

Objectifs:
- Proposer un modèle de gestion des risques informationnels et faire des recommandations.
- Définir et identifier le risque informationnel.
- Lister les moyens employés par les organismes pour la gestion des risques informationnels.

Méthodologie:
Revue de littérature confrontée à des interviews récoltées dans 5 institutions en Suisse Romande (institut de recherche et éducation, département de sécurité, banque, organisation internationale, HUG)



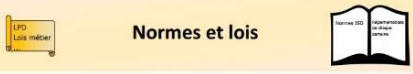


Aspects traités

Types de risques informationnels

Comment les classer?

Traitement



Place de la gestion des risques informationnels dans l'organisation de l'entreprise

L'information dans l'entreprise [2]

Information de fonctionnement - indispensable au fonctionnement «mécanique » quotidien de l'entreprise

Information d'influence - liée à la communication de /sur l'entreprise (orale, écrite, interne, externe)

Information d'anticipation - information stratégique qui permet à l'entreprise de voir venir certains changements de son environnement socio-économique dans le but d'en tirer un avantage un éviter un risque (veille, signaux faibles)

Résultats partiels:
- Les risques informationnels entrent souvent dans d'autres catégories de risques (opérationnels, informatiques, juridiques, etc.) et sont simplement listés ou classés selon plusieurs critères: la cause, la conséquence ou impact, par rapport à des activités ou domaines, etc.
- Le risque informationnel implique plusieurs départements dans une institution. C'est un risque transversal qui ne semble pas être nommé, ni géré en tant que catégorie de risque à part entière.

Bibliographie: [1] Adapté de WILDHABER, Bruno et al., 2016. *Information Governance: A Practical Guide. [en ligne]. Zurich: KRM. ISBN 978-3-9524430-2-6 [Consulté le 10 avril 2017].*
[2] LESCA, Elisabeth et LESCA Humbert, 2010. *Gestion de l'information.* 2e éd. Cormelles-le-Royal : EMS Editions. ISBN 978-2-84769-130-6

Master en Sciences de l'information - Décembre 2017
Giselle Castelo et **Monika Bolliger**
Projet de recherche supervisé par la prof. Basma Makhlouf Shabou