UNIVERSITÉ DU QUÉBEC

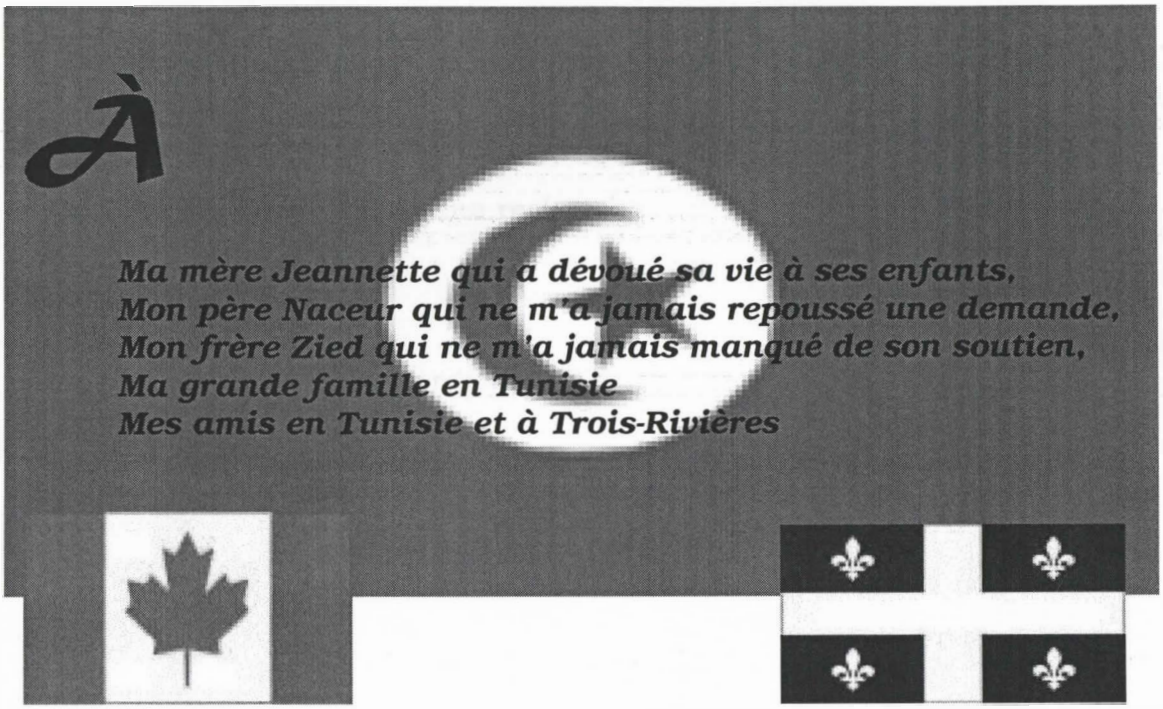
MÉMOIRE PRÉSENTÉ À
L'UNIVERSITÉ DU QUÉBEC À TROIS-RIVIÈRES

COMME EXIGENCE PARTIELLE
DE LA MAÎTRISE EN GESTION DE PROJET

PAR
Walid LABIDI

LA GESTION DU RISQUE ASSOCIÉ AUX PROJETS D'INFORMATISATION EN ENTREPRISES

MARS 2005


À
Ma mère Jeannette qui a dévoué sa vie à ses enfants,
Mon père Naceur qui ne m'a jamais repoussé une demande,
Mon frère Zied qui ne m'a jamais manqué de son soutien,
Ma grande famille en Tunisie
Mes amis en Tunisie et à Trois-Rivières

Remerciements

Je voudrais sincèrement remercier ma directrice de recherche, Mme Éliane Moreau pour les nombreux conseils qu'elle m'a donnés tout au long de la rédaction de ce travail. Son expérience et sa compétence m'ont aidé à mener à terme ma recherche.

SOMMAIRE

Dans ce travail de recherche, nous proposons d'étudier la théorie de gestion des risques relatifs aux projets d'informatisation en entreprises notamment la technologie Internet et ses dérivées. La problématique managériale réside dans les effets néfastes que peuvent avoir les risques sur l'avancement du projet en cas de leur réalisation. En effet, l'entreprise peut subir de pertes importantes liées aux coûts et à la perte de rentabilité dans le cas où elle ne gère pas convenablement l'ensemble des risques qu'elle rencontre. Dans un premier temps, nous procédons à la classification de ces risques. De plus, nous ferons le point sur les apports de certains auteurs au sujet de la gestion du risque. Nous définissons également un processus standard composé de cinq étapes dédiées à l'optimisation de la prévention contre risques durant le déroulement du projet. Les étapes composant le processus comportent certaines activités qui visent la planification de la politique de gestion du risque, l'identification des risques, l'analyse des impacts qu'ils peuvent avoir sur le projet d'informatisation, l'emploi d'une stratégie de réponse aux risques et enfin le suivi du processus. Sur un autre plan, nous justifions la nécessité de la présence de trois facteurs clefs de succès, à savoir, le soutien de la direction, le choix des critères de sélection de la technologie et la gestion de la structure d'organisation du projet. Par la suite, et dans le cadre des objectifs spécifiques de notre travail de recherche qui portent sur les risques inhérents à la technologie Internet et ses modes de gestion, nous identifions les principaux risques, et ce, à partir des apports théoriques de certains auteurs.

Dans la partie empirique de ce travail, nous effectuons des descriptions de cas basées sur des entrevues semi dirigées avec les responsables de certaines organisations québécoises ayant implanté la technologie Internet. Ces entrevues semi dirigées aideront à explorer d'autres catégories de risques et à comprendre les approches déployées par ces dernières. Les résultats auxquels nous avons aboutis démontrent le fort engagement de la part de nos répondants à acquérir les nouvelles technologies et à les ajuster par rapport aux orientations stratégiques de la compagnie. Dans ce cadre, nous avons noté plusieurs formes de soutien de la part des firmes interrogées. De plus, nous avons identifié certaines pratiques de sélection appliquées par ces dernières. Sur un autre plan, la gestion de la structure d'organisation du projet est basée sur la

répartition appropriée des responsabilités entre les participants au projet permettrait de prévenir toutes sortes de conflits. Les entrevues effectuées nous ont permis également d'approfondir le recensement des risques. Dans ce cadre, nos répondants ont souligné principalement la présence de risques relatifs à la définition du contenu de la technologie, l'adhésion et la collaboration des utilisateurs, l'engagement financier du client et la gestion des différences culturelles dans le cadre des projets d'informatisation menés à l'échelle internationale.

Quant à l'application du processus théorique de gestion du risque, nos résultats démontrent une forte attention qu'accordent les dirigeants interrogés à la planification de la politique de gestion du risque, en particulier à la préparation des ressources humaines et à la spécification de la technologie. Toutefois, les efforts au niveau de l'identification des risques mettent l'accent sur les rencontres régulières entre les intervenants au projet. Par ailleurs, les stratégies souvent privilégiées par nos répondants sont l'évitement et le transfert des risques à une autre partie en vue de les gérer telle que la sous-traitance ou l'assurance. Au niveau du suivi des risques, il y a souvent recours aux rapports d'état et aux audits de la part des experts. Enfin, cette étude est susceptible d'être approfondie, et ce, en se penchant davantage sur la gestion risque lié à l'existence de différences culturelles au sein des équipes de projet.

TABLE DES MATIÉRES

TABLE DES FIGURES

LISTE DES TABLEAUX

CHAPITRE I: INTRODUCTION

Ce travail de recherche se consacre à l'étude de la théorie de gestion du risque inhérent aux projets d'informatisation en entreprises. En effet, nous assistons actuellement à une multiplication de ces projets qui font intervenir plusieurs ressources humaines, matérielles et financières. Toutefois, il est clair que les risques spécifiques aux projets d'informatisation sont multiples et se présentent sous différentes formes. Par conséquent, il importe de s'attarder aux moyens menant à l'identification et à la mitigation de ces risques. C'est dans cette perspective que s'inscrit notre recherche. En effet, nous proposons une approche de gestion du risque basée sur la détermination des facteurs clefs de succès de toute politique de gestion du risque ainsi que la définition d'un processus comprenant les étapes à suivre dans l'objectif de gérer ces risques.

1.1 PROBLÈME MANAGÉRIAL

Issues de l'essor de l'informatique et des média, les technologies de l'information connaissent aujourd'hui un développement accéléré dans la production comme dans les services. Outre les nouvelles activités dont elles sont porteuses, les technologies de l'information jouent un rôle majeur dans le processus de mutation des entreprises. C'est pour cette raison que nous porterons notre attention dans le cadre du présent travail de recherche aux risques que rencontrent les projets visant le développement de ces technologies étant donné l'importance qu'elles occupent au sein des entreprises de nos jours. D'ailleurs, les risques sont multiples et de différentes natures. Ainsi, nous présenterons les différentes catégories des risques et les modes de leur gestion.

En effet, pour connaître leur état, coordonner leurs processus ou planifier leurs décisions, les organisations disposent d'un certain nombre de technologies d'information (Darracott, 2003). Leur mise en place requiert des investissements de la part de l'organisation et des efforts successifs de la part des cadres, des usagers et des spécialistes du traitement des données. Ainsi, à tout moment de son histoire, une organisation dispose d'un portefeuille de technologies d'information dont le niveau respectif de développement varie grandement.

Actuellement, plusieurs facteurs contribuent à l'expansion des technologies d'information. Selon Benaroya et Landau (1999), l'environnement des entreprises change constamment et l'ouverture des marchés est devenue une réalité pour ces dernières. « La mondialisation devient l'actualité de tous, même des plus petites entreprises. Pour tous, les contraintes sont les mêmes : aller plus vite, innover, s'adapter, fournir un meilleur service » (Deming, 1996). Il s'agit d'une évolution rapide de l'environnement caractérisée par plusieurs changements significatifs au niveau de la concurrence entre les entreprises qui devient de plus en plus rude (pression sur les coûts, contraintes de rentabilité encore plus fortes, etc.). Plus, encore, Godes, Ofek et Sarvary (2003) voient que l'acharnement de la concurrence a permis d'introduire plus de sophistication technique au niveau des produits. Dans cette perspective, les entreprises auront davantage recours aux technologies de l'information dans l'objectif de diversifier leurs produits sur le plan technique. Cela explique en quelque sorte la rapidité des avancées technologiques allant de pair avec un accroissement de la complexité et de la diversité des produits de nos jours.

Sur un autre plan, Aubert et Dussart (2002) pensent que le recours aux nouveaux systèmes d'entreprise par les dirigeants peut s'expliquer aussi par un souci d'intégration. En effet, il est parfois indispensable et rentable d'intégrer les systèmes d'information à l'échelle de l'organisation. Il s'agit d'intégrer les processus d'affaires clés d'une entreprise en un seul système ou logiciel pour que l'information puisse circuler d'une façon transparente au sein de l'organisation. Par conséquent, une stratégie d'intégration soutenue par des technologies appropriées permettra d'améliorer la coordination, l'efficacité et la prise de décision au sein de l'entreprise.

En conséquence, et face à ces exigences, les entreprises doivent acquérir les moyens technologiques appropriés. Dans ce sens, des auteurs tels que Marchewka (2003), Aboubekr et Rivard (2002) et Laudon et Laudon (2000) affirment que l'implantation de technologies de l'information pourrait apporter des réponses aux problématiques posées aux entreprises : nouveaux types de relations clients, gains de parts de marché, création de nouveaux débouchés pour les produits, vitrine mondiale, information fiable et rapide, mise à jour de base de données, etc.

En général, l'ensemble des processus d'une organisation dépend de la façon dont l'information y est acheminée. Selon Bacca (2001), la répartition des responsabilités permet d'améliorer l'efficacité de l'entreprise. Dans ce sens, la circulation des flux d'informations sert à coordonner et à synchroniser les différentes opérations faisant partie d'un même processus. Ces flux d'informations prennent progressivement la forme de messages, de fichiers, de procédures. Afin d'être acheminés convenablement, l'acheminement des flux d'informations requiert des ressources de la part de l'organisation telles que des hommes, des machines, du temps, de l'argent, etc.

Les apports des technologies de l'information sont indéniables pour les organisations. Elles offrent des leviers de performance dans de multiples directions. Elles forment ainsi des outils et instruments au service des objectifs aussi bien stratégiques qu'opérationnels de l'entreprise, et ce, en favorisant l'échange, la réactivité et le changement (Rondeau, 2001). L'utilisation de ces technologies d'information offre donc à l'organisation des outils de collaboration, de communication et de coordination (Godes, Ofek et Sarvary, 2003). Laudon et Laudon (2000) confirment ce constat en précisant que la croissance accrue des technologies de l'information a permis la création de réseaux de communication puissants. Ces réseaux permettent aux organisations d'accéder à des bases de données gigantesques partout dans le monde et de coordonner leurs activités dans l'espace et dans le temps.

Par ailleurs, il y a lieu de mettre l'accent sur la forte croissance qui caractérise le développement de technologies d'information. En effet, l'industrie de l'informatique est une des plus dynamiques dans le monde des affaires tant au niveau de la production qu'au niveau de la diversité (Aubert et Dussart, 2002). Les entreprises partout dans le monde ont recours aux nouvelles innovations pour fructifier des apports bénéfiques déjà mentionnés ci haut. Waltner (1999) note que les innovations dans le domaine des applications logicielles et progicielles[1] représentent l'un des principaux piliers de n'importe quelle entreprise qui en fait recours. Également, Buttrick (2002) précise que le développement de la technologie Internet, y compris

[1] Selon la définition de Laudon et Laudon (2000), les progiciels sont des programmes pré-écrits et préprogrammés offerts sur le marché et qui rassemblent un ensemble de logiciels destinés à la gestion de certaines fonctions au niveau de l'organisation.

les dérivées à savoir les réseaux Intranet et Extranet, suscite de plus en plus l'attention des dirigeants des organisations en raison des nombreuses opportunités qu'il crée. En effet et selon les observations de Ward (2003), l'Internet permet aux organisations de diminuer le coût des communications, de réduire le coût des transactions, de personnaliser les produits et d'accélérer la diffusion des connaissances. C'est pour l'ensemble de ces raisons que dans le cadre du travail de recherche présent, nous aurons un regard particulier à la technologie Internet.

En effet, d'autres fonctions dérivent de l'utilisation d'Internet dont principalement l'Intranet, l'Extranet et le commerce électronique. Voici quelques définitions dans ce qui suit:

1. **L'Internet et le commerce électronique :** L'Internet a créé une plate-forme universelle pour l'achat et la vente de biens. Sa technologie procure également diverses fonctionnalités pour la mise en œuvre de processus d'affaires importants à l'intérieur de l'entreprise et pour la liaison électronique de ces processus à ceux des autres entreprises. En effet, l'Internet devient rapidement le fondement du commerce électronique car il offre aux entreprises une manière encore plus simple et économique de se relier avec d'autres organisations et personnes. Les sites Web sont accessibles 24 heures par jour et permettent la création de nouveaux circuits de mise en marché et le recours au marketing interactif avec les clients pour les entreprises (Laudon et Laudon, 2000).

2. **L'Intranet :** il s'agit d'un réseau interne à l'entreprise destiné à la gestion des connaissances et à la communication entre les différents échelons. Cette technologie permet une connectivité instantanée, en reliant tous les ordinateurs en un seul système de réseau. Les entreprises peuvent relier leurs Intranets à des bases de données, ce qui permet aux employés d'effectuer plus rapidement leurs opérations (Bacca, 2001 ; Marchewka, 2003).

3. **L'Extranet** : selon la définition adoptée par Marchewka (2003), l'Extranet est un réseau qui utilise la technologie Internet pour lier un ensemble de partenaires à l'organisation dont principalement ses clients, ses fournisseurs et ses principaux distributeurs. Les Extranets permettent dans ce sens de relier les Intranets relatifs aux partenaires en

question avec celui de l'organisation. En conséquence, une firme pourrait faire partie de plusieurs Extranets en même temps.

Comme nous l'avons mis en relief dans les paragraphes précédents, l'implantation des technologies d'information est de plus en plus courante dans les organisations. Si les bénéfices potentiels attachés à ces solutions sont importants, les risques sont à l'avenant. Plusieurs projets ont été abandonnés ou ont entraîné des conséquences graves pour les organisations ayant amorcé ces initiatives. Sans une gestion adéquate, l'implantation d'un système d'information prendra plus de temps et dépassera le budget alloué. En effet, un projet d'informatisation mal géré mènera aux problèmes suivants (Laudon , Laudon , 2000) :

1. Dépassement des coûts
2. Dépassement des échéances
3. Problèmes techniques entravant la performance
4. Impossibilité d'obtenir les bénéfices escomptés

Dans ce cadre, Cosgrove (2001) note que 31% des entreprises ayant participé à une enquête sur l'implantation de solutions d'affaires, notait que leurs projets avaient dépassé leur budget, alors que 36% dépassent leurs échéances. Ces résultats correspondent à ceux du Gartner Group qui estime que 40% des entreprises implantant des solutions intégrées dépasseront leurs budgets de plus de 50% (Zrimsek, Phelan, Karamouzis et Frey, 2001).

Cela fait intervenir la notion du risque. Le risque et la gestion du risque sont des sujets qui ont été abordés dans plusieurs domaines comme l'assurance, l'économie, le management, la médecine et l'ingénierie. Dans chaque domaine, on évalue le risque selon l'objet de l'analyse, ce qui mène à l'adoption de différentes approches concernant le risque et ses modes de gestion.

Dans certaines situations, le risque est perçu comme étant un événement négatif. Barki, Rivard et Talbot (1992) définissent le risque comme « un événement qui, s'il survient, représentera une menace au patrimoine d'une entité économique.» Faisant recours à cette

définition, les risques sont des événements indésirables qui peuvent survenir. Appliquée dans le contexte de la gestion de projet, l'entité économique peut être une organisation.

La finance a adopté différentes définitions du risque qui s'obtient en calculant la variance de la distribution des flux financiers. Le risque est défini comme étant la volatilité de la valeur d'un portefeuille (Levine, 1975). La gestion du risque sous-tend l'arbitrage entre le risque et les revenus. Pour un certain niveau de revenu, les dirigeants préfèrent une faible volatilité. Toutefois, ils peuvent être favorables à tolérer un plus grand niveau de volatilité dans la mesure où les revenus escomptés seront plus importants (Schirripa et Tecotzky, 2000). Selon Boehm (1989), la valeur du risque lié à un projet d'informatisation se définit ainsi :

*Probabilité (CI) * Perte (CI)*
Où CI représente la conséquence indésirable

Pour Buttrick (2002), la détermination des risques est importante dans la mesure où les commanditaires potentiels du projet demandent souvent de connaître tous les risques y afférents avant de prendre toute décision à son égard. Bien évidemment, les risques sont de diverses nature, les plus importants et fréquents étant les suivants : le risque financier, le risque technique, le risque de coût et le risque d'échéanciers (Barki, Rivard, et Talbot, 1992 ; Laudon et Laudon, 2000 ; Aboubekr et Rivard, 2002 ; Aboubekr et Rivard, 2003 ; Franklin Jr., 1997 et Marchewka, 2003).

La détermination de l'ensemble des risques inhérents aux projets d'informatisation nous introduit à la notion de gestion du risque et nous amène sur un autre plan à constater l'importance de cette dernière dans les entreprises d'aujourd'hui. En effet, il est souvent rare que les estimations se concrétisent dans la réalité, étant donné que le projet est appelé à composer avec un environnement dynamique. Plusieurs auteurs dont Jones (1994), Buttrick (2002), Aboubekr et Rivard (2002), Aboubekr et Rivard (2003), Nelson (1999) et Marchewka (2003) pensent que la gestion du risque permet d'identifier, d'analyser et de développer des stratégies destinées à composer efficacement avec le risque couru par le projet. Cela implique alors pour les organisations la nécessité de penser à la manière idéale pour le développement des technologies

d'information. Il s'agit d'opter pour un modèle de gestion du risque susceptible de constituer une réponse appropriée aux risques auxquels fait face tout projet d'informatisation au sein des organisations. Un tel modèle doit proposer des moyens susceptibles de réduire l'envergure de ces risques et de les isoler.

1.2 OBJECTIFS SPÉCIFIQUES DE LA RECHERCHE

Nous avons mentionné dans ce qui précède l'importance relative qui devrait être rattachée à la technologie Internet, y compris les réseaux dérivés à savoir l'Intranet et l'Extranet, du fait du grand essor qu'elle connaît. Les risques relatifs à la technologie Internet sont multiples et requièrent de l'attention de la part des dirigeants des entreprises. Par conséquent, la détermination de ces risques spécifiques aux réseaux Internet, Intranet et Extranet ainsi que leurs modes de gestion, représentent les objectifs spécifiques de ce travail de recherche.

Dans le cadre des projets de développement de réseaux de communication (Internet, Intranet et Extranet), quels sont les risques relatifs au développement de ces technologies et les outils destinés à leur gestion ? Par ailleurs, comment les principes de la gestion du risque inhérent au développement de réseaux de communication sont-ils appliqués dans les firmes québécoises ?

1.3 PLAN DE LA RECHERCHE

Dans le présent travail de recherche, nous expliciterons dans le prochain chapitre les principaux risques reliés à l'implantation des technologies de l'information dans les processus d'affaires des organisations, et nous introduirons également la notion de gestion du risque ainsi que la dynamique des risques. Ensuite, nous avancerons un modèle élaboré par Marchewka (2003) pour la gestion du risque inhérent au développement des technologies au sein des organisations. Dans le cadre de ce modèle, nous développerons certains outils avancés par certains auteurs dans l'objectif de contrer l'effet des risques et d'en minimiser l'importance comme l'assurance, la sous-traitance et le développement par l'utilisateur final. De plus et dans le

cadre des objectifs spécifiques de notre recherche, nous présenterons dans ce chapitre une illustration des risques associés à l'implantation de la technologie Internet et de ses dérivées, dans les organisations. Ainsi, nous tenterons de déterminer les principaux risques inhérents aux réseaux Internet ainsi que les méthodes et les outils appropriés quant à leur gestion. Le troisième chapitre sera consacré à la présentation de la méthodologie de recherche qui comprend la discussion de la nature de la question de recherche de ce mémoire, la méthode de collecte de données, l'échantillonnage et le traitement des résultats. Dans le quatrième chapitre, nous appliquerons la théorie avancée par les auteurs en effectuant une série d'études de cas appuyées par des entrevues en profondeur, et ce, auprès de certains organisations ou entités économiques ayant déjà implanté des réseaux de communications basés sur la technologie Internet. Enfin, nous mettrons en relief les différents points saillants de ce travail de recherche dans le cadre de la conclusion générale. Également, nous discuterons les limites de cette étude et nous présenterons nos recommandations ainsi que les voies futures de recherche.

CHAPITRE II : CADRE THÉORIQUE DE LA GESTION DU RISQUE DES TECHNOLOGIES D'INFORMATION

Nous avons déjà pu constater dans l'introduction à travers les contributions de plusieurs auteurs, l'importance pour les organisations d'avoir recours aux technologies d'information et de les introduire dans leur fonctionnement. En effet, les dirigeants ne peuvent pas passer outre les innovations étant donné le rôle crucial qu'elles jouent dans les organisations d'aujourd'hui. Les technologies exercent une influence directe sur les mécanismes de prise de décision et de planification au sein des entreprises. Dans ce sens, Aubert et Dussart (2002) avancent que la forte croissance que connaît le domaine de l'informatique a permis d'intégrer les processus d'affaires de plusieurs entités même si elles sont distinctes.

Toutefois et malgré les apports bénéfiques de ces technologies pour les organisations, plusieurs risques sont associés à leur développement. Par conséquent, les organisations sont appelées à bien gérer l'ensemble de ces risques. Selon Greenstein et Vasarhelyi (2002), la gestion du risque est une méthodologie qui vise l'évaluation de la probabilité d'occurrence de certains événements pouvant avoir divers impacts. Qui plus est, la gestion du risque prévoit la mise en place de stratégies appropriées pour composer avec ces risques. Pour Mantel et Meredith (2000), la contribution principale de la gestion du risque serait de centrer l'attention des preneurs de décision sur certains paramètres imprévisibles qui rentrent dans le processus de prise de décision.

Cependant, il est important de bien connaître les différents risques liés au développement des technologies d'information, et ce, afin de pouvoir agencer les moyens nécessaires en vue de les contourner. Selon Buttrick (2002), la détermination des risques permet au chef de projet d'établir un ordre de priorité pour l'exécution des activités risquées. Une telle démarche permet de préserver une marge de manœuvre suffisante pour une correction ultérieure. Ainsi, le chef de projet sera en mesure d'éviter tout retard dans la réalisation du projet qui soit dû aux activités risquées. Dans ce chapitre dédié au cadre conceptuel de notre étude, nous présenterons dans une première section les principaux risques associés aux projets d'informatisation au sein des organisations. La deuxième section se consacrera à la théorie de la gestion du risque, tandis que la troisième section énumèrera les différents facteurs clefs de succès de toute politique de gestion

du risque. Enfin, dans la quatrième section nous présenterons le modèle théorique que nous avons adapté de Marchewka (2003), et qui consiste en un processus de gestion du risque composé de cinq étapes que nous expliciterons.

2.1 Les différents risques associés au développement des TI au sein des organisations

Les risques sont de différentes natures. Tout d'abord, le volet finance représente la composante la plus importante de tout projet. En effet, les questions de profit et de rentabilité de la technologie représentent l'objectif le plus recherché par les organisations. Par la suite, nous nous concentrons sur le risque technique qui représente une grande préoccupation pour les responsables du développement de la technologie. En effet, plusieurs problématiques d'ordre technique que nous soulèverons dans ce qui suit, suscitent l'intérêt de ces responsables et demandent une réponse appropriée. Viennent après successivement les risques de coût et d'échéancier, qui, même s'ils sont d'une importance relativement moins éminente, demandent néanmoins de l'attention et du suivi. Cette typologie des risques relatifs aux projets d'informatisation a été proposée par des auteurs tels que Karolak (1996), Laudon et Laudon (2000) et Barki, Bourdeau et Rivard (2003). Ces auteurs affirment que les projets d'informatisation rencontrent très souvent ces catégories de risques.

2.1.1 Risque financier

Les technologies d'information permettent aux organisations de devancer la concurrence en influençant les buts, les opérations, les produits, les services et les relations avec l'environnement. Toutefois, les coûts initiaux inhérents à l'implantation des TI sont élevés. Les avantages concrets sont cependant vagues à la phase initiale. Les avantages ne peuvent être évalués qu'une fois les employés sauront fonctionner la technologie mise en place et utiliser de nouvelles connaissances au niveau des opérations.

Il est évident que la rentabilité fait l'objet de la plus importante question soulevée lors de la réalisation d'un projet d'informatisation. La technologie n'est pas censée produire des avantages stratégiques durables puisque les concurrents ont accès à une vaste gamme de technologies sur le

marché. Cependant, le recours aux technologies d'information dans le but de mieux gérer les activités et de mieux répondre à la clientèle représente un atout exclusif à l'organisation. Il serait donc impératif pour les gestionnaires de savoir comment utiliser les technologies dans le but de générer de la valeur pour l'organisation (Laudon et Laudon, 2000).

Néanmoins, la rentabilisation des technologies nouvellement implantées nécessite que l'on accorde une grande attention aux défaillances techniques et aux moyens appropriés destinés à les éviter ou à les minimiser. Dans la sous section qui suit, nous mettons l'emphase sur les principaux risques d'ordre technique auxquels fait face l'équipe de projet lors du développement de technologies.

2.1.2 Risque technique

Chang et Gable (2001) et Clemons (1995) préconisent que dans la majorité des cas, les échecs de l'implantation des technologies d'information sont dus à une mauvaise qualité du système. La mauvaise qualité peut en effet être en relation avec les fonctionnalités qu'offre la technologie ou avec les problèmes techniques qui se manifestent suite à l'implantation. Ces auteurs ont remarqué que la performance observée de certains systèmes ne reconnaît pas les exigences opérationnelles des entreprises qui les déploient. Les risques techniques sont associés à la performance de la TI. La notion de performance englobe les éléments suivants (Karolak, 1996) :

1) Les fonctionnalités : la capacité de la TI à respecter les fonctions énoncées.
2) La qualité : la capacité de la TI à répondre aux exigences de l'utilisateur final.
3) La crédibilité : la capacité de la TI à opérer sur une longue durée sans commettre d'erreurs.
4) La maniabilité : la capacité de la TI à être entretenue facilement.
5) La transférabilité : la capacité de la TI à être réutilisée pour une application similaire ou même différente.

Chacun de ces éléments est relié au risque de performance. Toutefois, l'ampleur du risque technique est en fonction de la perception des utilisateurs finaux et de la direction. De plus, le risque est évalué par rapport aux critères de performance déterminés lors de la conception de la TI (Karolak, 1996). Sur un autre plan, il importe que la technologie implantée soit ajustée par rapport aux systèmes légués[2] ainsi qu'aux processus d'affaires de l'organisation. Les dirigeants ne peuvent pas être certains de la capacité de la TI implantée à échanger des données avec les systèmes déjà en place (Laudon et Laudon, 2000).

Le risque technique est déterminé par rapport au seuil de performance prédéfini. Dans ce sens, des éléments de la performance de la TI sont déterminés par les attentes de l'utilisateur final. Qui plus est, les ressources disponibles lors de la réalisation du projet d'informatisation ont une part dans la détermination du seuil de performance. En effet, il serait fatal pour l'organisation de concevoir un système d'information qui ne prend pas en considération les attentes des utilisateurs finaux. L'interface utilisateur, qui désigne la partie visible aux utilisateurs de la technologie, peut être mal conçue. Parfois, les spécialistes adoptent une démarche de résolution des problèmes très technique. Ils recherchent des solutions techniques perfectionnées qui optimisent l'efficacité du matériel et du logiciel aux dépens de la convivialité ou de l'efficacité pour l'organisation. Quant aux utilisateurs, ils préfèrent des systèmes axés sur la résolution des problèmes et la simplification des tâches organisationnelles.

Les projets d'informatisation sont souvent voués à l'échec lorsqu'il y a une telle divergence entre les deux groupes : concepteurs et utilisateurs (Laudon et Laudon, 2000). La conséquence logique d'une conception non adaptée aux besoins des employés seraient la démotivation, les fautes dans l'exécution des tâches et même un climat de conflits et d'instabilité dans l'organisation.

Sur un autre plan, Nelson (1999) rappelle qu'avec les moyens traditionnels de communication, les informations s'adressaient à des personnes bien déterminées, tandis que, avec l'essor révolutionnaire de nouveaux outils technologiques de communication, le contenu est

---

[2] Selon la terminologie utilisée par Laudon et Laudon (2000), les systèmes légués sont les technologies déjà opérantes dans l'entreprise. L'équivalent en anglais étant « Legacy systems. »

disponible pour tout le monde. En effet, Franklin Jr. (1997) avance que les firmes d'aujourd'hui ont à composer à distance avec des partenaires virtuels. De plus, Marchewka (2003) rappelle que les ressources informatiques aussi bien logicielles que matérielles, font face constamment à des menaces d'attaques – aussi bien internes qu'externes à l'organisation. Ces attaques sont susceptibles de causer un certain nombre de problèmes. En effet, ces programmes peuvent être altérés jusqu'à ce qu'ils deviennent inopérants. Ainsi, Nelson (1999) ainsi que plusieurs auteurs, tels que Franklin Jr. (1997) et Marchewka (2003) soulèvent la question de la sécurité des réseaux et des moyens appropriés permettant de la résoudre.

En guise de conclusion, la sous-estimation de l'ensemble ou d'une partie de ces risques est susceptible d'induire certains problèmes à savoir principalement le dépassement de coûts relatifs aux révisions et aux corrections requises. En effet, le fait de corriger fréquemment les défaillances et les défauts techniques de la technologie serait de nature à causer d'énormes coûts supplémentaires. Dans ce qui suit, nous élucidons les éléments de coûts devant être surveillés lors du développement des technologies au sein des organisations.

2.1.3 Risque de coût

Le dépassement du budget constitue une contrainte qui entrave la réalisation des projets d'informatisation. Selon l'enquête effectuée par Cosgrove en 2001, le budget serait dépassé de 38% en moyenne auprès des entreprises ayant implanté des progiciels de gestion intégrée.

Les risques de coût sont corrélés au coût de la TI durant son processus de développement. Le coût de la TI englobe les aspects suivants identifiés par Karolak (1996) :

1) Le budget : la capacité à développer un système ou une TI en se limitant à un certain montant d'argent préalablement déterminé par la direction.
2) Les coûts réversibles : la capacité à identifier et à gérer les coûts relatifs au support du processus de développement de la TI comme les facilités et les coûts de maintenance.

3) Les coûts irréversibles : la capacité à identifier et à gérer les coûts relatifs au développement initial de la TI (investissement en capital).
4) Les coûts fixes : il s'agit des coûts dont la variation ne peut être rattachée à la capacité de production.
5) Les coûts variables : ce sont par contre les coûts liés à la cadence de production. Leur évolution suit l'évolution de la production.
6) Les marges de profit/perte : la capacité de prédire et de contrôler la marge de profit espérée de la TI. Cela relève du réalisme de la direction qui fait appel à sa capacité à estimer le coût total de son investissement, étant donné certaines hypothèses établies au départ.

Chacune de ces questions est liée au risque de coût de la technologie. L'identification, l'évaluation et la prédiction des risques de coût auront une influence certaine sur le déroulement du projet d'informatisation. Par ailleurs, nous signalons que les risques de coût sont déterminés par d'autres éléments tels que la disponibilité des fonds et les attentes de la direction. Les risques de coût peuvent survenir même après l'implantation des TI surtout s'ils font appel à des technologies sophistiquées lors de leur utilisation. Cela expose les TI implantées au risque de bris ou de mauvaise manipulation. Un tel risque peut engendrer selon l'envergure de l'investissement des coûts énormes et difficiles à surmonter par l'organisation (McLaughlin, 2003).

Bien évidemment, le dépassement de coût peut induire un retard dans l'achèvement du projet. En effet, tout retard dans l'exécution est synonyme de charges supplémentaires pour le projet. Ainsi, nous sommes en mesure de noter la présence d'une hiérarchie descendante des risques (Risque technique $\Longrightarrow$ Risque de coût $\Longrightarrow$ Risque d'échéancier).

2.1.4 Risque d'échéancier

Martin (1998) avance que la majorité des entreprises ne respectent pas les échéanciers durant la réalisation d'un projet d'informatisation. Keil, Mann et Ray (2000) soulèvent la grande corrélation existant entre le dépassement de l'échéancier et le dépassement du budget. En effet, tout retard dans l'exécution engendre plus de coûts aussi bien fixes que variables.

Le risque d'échéancier regroupe les éléments suivants (Karolak, 1996) :

1) La flexibilité : la capacité de l'échéancier établi à être soit compressé soit élargi selon les durées respectives requises pour l'exécution des tâches.
2) La rencontre des jalons établis : la capacité de l'organisation à rencontrer les jalons établis lors du découpage du projet.
3) Le réalisme : la capacité de l'échéancier à répondre aux attentes des utilisateurs, de la direction et des concepteurs avec efficacité.

Les éléments liés à l'échéancier représentent des facteurs influençant la performance de la technologie implantée. Par exemple, il y a toujours une corrélation entre le retardement de l'échéancier et le coût total d'implantation. Dans cette perspective, une corrélation similaire semble exister entre le raccourcissement de l'échéancier et l'accroissement des problèmes techniques qui surviennent après l'implantation. Ces problèmes sont identifiés par les utilisateurs plutôt que par les concepteurs.

Comme les risques de coût, les risques d'échéancier ne sont cernés qu'après la fin de l'implantation de la TI. Par conséquent, ce risque persiste tout au long du processus de développement de la TI. Les risques d'échéancier sont fonction d'autres facteurs comme la disponibilité de la technologie nécessaire, du personnel, du financement ou même le changement d'envergure de la TI au cours du processus de son développement.

Tableau 1: Récapitulatif des risques relatifs aux projets d'informatisation

Risque	Caractéristiques	Auteurs afférents
Financier	➢ Difficultés dans la prévision des bénéfices attendus de l'investissement. Cela rend difficile l'établissement des études de rentabilité par rapports aux coûts engagés. ➢ Le risque financier concerne aussi la capacité de l'organisation a rentabiliser la technologie implantée et a générer des avantages stratégiques.	Laudon et Laudon (2000) ; Mantel et Meredith (2000) ; Pradels (1981) ; ARTE (1986) ; Paquin (1990) ; Chokron (1996) ; O'brien (1995) et Porter (1980)
Technique	➢ Mauvaise qualité de la technologie ➢ La performance observée et les fonctionnalités de la technologie ne correspondent pas aux exigences de l'activité de l'entreprise. ➢ La technologie nouvellement implantée ne concorde avec aux systèmes légués dans l'entreprise. ➢ La technologie développée ne prend pas en considération les attentes de l'utilisateur final.	Chang et Gable (2001) ; Clemons (1995) ; Karolak (1996) ; Laudon et Laudon (2000), Nelson (1999) ; Franklin Jr. (1997) ; Marchewka (2003) ; Pradels (1981) ; ARTE (1986) ; Paquin (1990) ; Chokron (1996) ; O'brien (1995) ; Porter (1980) et Laudon et Laudon (2000)
De coût	➢ Difficultés dans la prévision des coûts du projet. ➢ Le dépassement du budget alloué au projet. ➢ Des mauvaises manipulations de la part des utilisateurs qui peuvent causer des coûts supplémentaires.	Karolak (1996) ; ARTE (1986) ; Paquin (1990) ; Chokron (1996) ; O'brien (1995) ; Porter (1980) et Laudon et Laudon (2000)
D'échéancier	➢ De faux jugements lors de la détermination de l'échéancier du projet ainsi que des différents jalons devant être rencontrés durant le projet. ➢ Des échéanciers non flexibles et qui ne prévoient pas les changements accidentels au niveau de certaines tâches du projet.	Martin (1998) ; Keil, Mann et Ray (2000) ; Karolak (1996) ; Laudon et Laudon (2000), Nelson (1999) ; Franklin Jr. (1997) ; Marchewka (2003) et Pradels (1981) .

Comme nous venons de le voir, il existe une multitude de risques susceptibles d'entraver la réalisation de tout projet d'informatisation. Ces risques dépendent d'une part du contexte caractérisant l'activité de l'entreprise, et d'autre part de l'efficacité de la politique qu'elle déploie en vue de les contourner. Par conséquent, cela implique la nécessité du recours à une politique

appropriée de gestion de risque. Dans ce cadre, Greenstein et Vasarhelyi, (2002) pensent que les gestionnaires de projet peuvent constater l'importance du recours aux pratiques de gestion du risque à travers les pertes subies dans le passé en raison de l'insuffisance des processus et/ou de la technologie qu'ils utilisaient.

2.2 La théorie de la gestion du risque

Le but de la gestion du risque est de planifier les événements indésirables d'une façon systématique. Les firmes peuvent mener une politique de gestion du risque de façon réactive ou proactive. Buttrick (2002) affirme que la détermination des risques est importante dans la mesure où les commanditaires potentiels du projet demandent souvent de connaître tous les risques y afférents avant de prendre toute décision à son égard.

A ce stade, il importe de préciser la hiérarchie des risques que nous adoptons dans le cadre des objectifs spécifiques de notre travail de recherche. Le niveau le plus haut de cette hiérarchie étant les risques de projet en général. Par la suite, il y a les risques relatifs aux projets d'informatisation. Enfin, les risques inhérents aux projets de réseaux Internet représentent le troisième niveau de cette hiérarchie. Évidemment, il existe des spécificités à chaque niveau de risque par rapport au niveau supérieur. En effet, ce qui est spécifique aux risques des projets d'informatisation ce sont les risques d'erreur de conception. Nous notons d'abord que les projets d'informatisation ont comme objectif de développer des solutions d'affaires informatiques pour l'entreprise en vue de faciliter la gestion d'une partie ou de l'ensemble de son activité (ex : base de données, Intranet, client/serveur, etc.) Dans le cadre de cette catégorie de projet, les risques techniques sont très présents dans la mesure où la solution proposée par les concepteurs doit correspondre parfaitement aux processus d'affaires de l'organisation. Parfois, la solution proposée ne tient pas compte de certaines particularités relatives au contexte de l'entreprise. Cependant, l'erreur peut survenir au moment du développement du concept. Également, les risques relatifs aux projets d'informatisation se caractérisent par la gravité des impacts qu'ils peuvent avoir. En effet, toute mauvaise manipulation de la technologie implantée risque de bloquer l'accès aux données et même l'activité d'exploitation de l'entreprise. En ce qui concerne les spécificités des risques des projets de réseaux Internet, l'élément qui se distingue le plus étant

le risque de piratage de données. En effet, la technologie Internet relie l'entreprise à un ensemble d'opérateurs en dedans et en dehors de ses frontières. Cependant, certains utilisateurs peuvent s'approprier de mauvaise foi des informations confidentielles, et ce, pour des usages illicites. Par ailleurs, d'autres formes de risques spécifiques aux projets de réseaux Internet seront explicitées davantage dans la section 2.4.2.2.

Selon Jones (1994), la gestion du risque requiert la présence de trois éléments essentiels, à savoir : le soutien et l'engagement des parties impliquées dans le projet (les hauts dirigeants, les clients, le gestionnaire et l'équipe de projet). Deuxièmement, chaque partie impliquée dans le projet doit reconnaître sa responsabilité dans la réalisation d'un risque donné. Des ressources doivent être mis à la disposition de ces personnes pour la prévision et la gestion des risques dont ils en sont les responsables. Troisièmement, il faut être conscient du fait que chaque type de projet à ses propres risques. Autrement dit, certains risques sont spécifiques à certains types de projets. Cependant, la gestion du risque peut aboutir également à des opportunités susceptibles d'avoir un effet bénéfique sur le projet. Le processus de gestion du risque permet donc d'éviter les événements indésirables et de saisir les opportunités (Buttrick, 2002). En effet, les opportunités interviennent de la même façon que les risques dans le cycle de vie du projet mais en ayant toutefois des incidences favorables au projet.

Par ailleurs, Greenstein et Vasarhelyi (2002) pensent qu'il est impossible d'éliminer tout le risque dans les projets d'informatisation. Buttrick (2002) soutient ce constat. Il préconise qu'une planification appropriée des risques permet de les minimiser. Cependant, Buttrick (2002) poursuit en affirmant que la gestion du risque ne peut aboutir en aucun cas à l'anéantissement total de ces risques. Choo (2001) tient à son tour à préciser que la gestion du risque des projets ne se donne pas comme objectif d'éliminer la totalité du risque mais plutôt de bâtir des décisions bien fondées en fonction des risques identifiés.

Marchewka (2003) distingue trois types de risques : connus, connus-inconnus, et inconnus-inconnus. Les risques connus sont ceux qui vont survenir avec certitude (Wideman, 1992). Quant aux risques connus-inconnus, l'incertitude en caractérise une partie. Par exemple, on est parfois sûr de l'occurrence du risque mais on ne connaît pas l'amplitude de son impact. Par ailleurs,

l'incertitude et l'imprévisibilité portent sur la totalité des risques inconnus-inconnus. C'est effectivement cette dernière catégorie de risques inconnus-inconnus qui constitue le risque résiduel relatif au développement des technologies d'information. Il s'agit pour Greenstein et Vasarhelyi (2002) d'un risque résiduel dû aux situations complètement imprévisibles ou dont les mesures de contrôle ne sont pas disponibles. La mise en place de mesures de contrôle additionnelles ne permet pas d'éliminer le risque résiduel qui varie d'une firme à l'autre. En effet, le risque est associé négativement au montant des coûts relatifs aux mesures de contrôle. La figure 1 présente ces niveaux de risques :

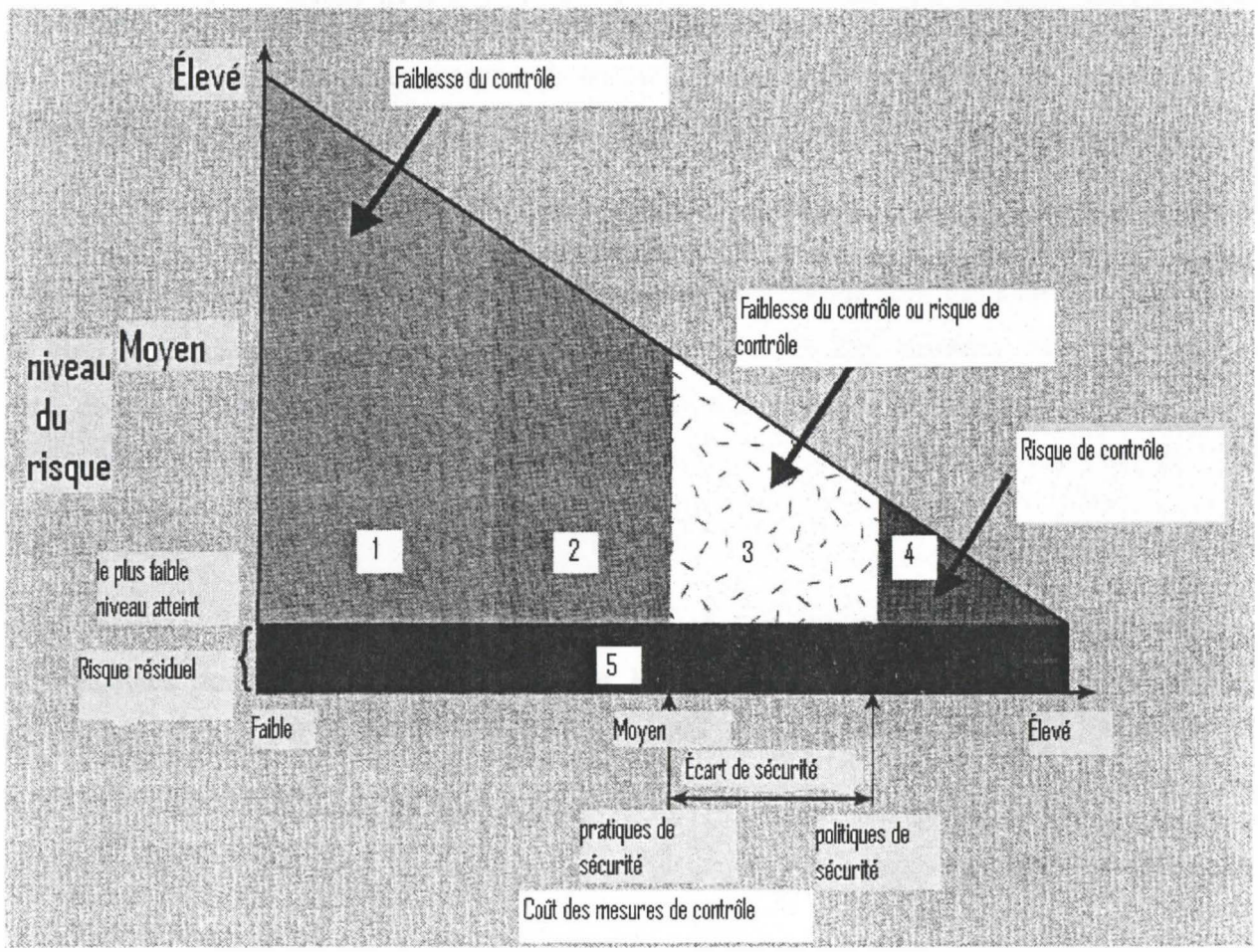


Figure 1 : Les niveaux du risque et leurs coûts relatifs (Greenstein et Vasarhelyi, 2002 : 254)

La zone *Faiblesse de contrôle*[3] (Zone 1) fait référence aux situations dans lesquelles les coûts relatifs aux mesures de contrôle du risque sont inférieurs aux bénéfices rattachés. Dans cette zone, toute dépense visant de mettre en place des mesures de contrôle aura incontestablement des effets positifs sur la réduction du niveau des risques. Tandis que la zone *Risque de contrôle*[4] (Zone 4), elle dénote la situation dans laquelle les bénéfices attendus peuvent ne pas dépasser les coûts de contrôle additionnels. Dans cette zone, l'investissement dans des mesures de contrôle additionnelles peut très probablement s'avérer inutile dans la minimisation des risques du fait qu'il est impossible de supprimer le risque résiduel (Zone 5).

Concernant la Zone 3, située entre *Faiblesse de contrôle* et *Risque de contrôle*[5], l'investissement additionnel dans des mesures de contrôle demande de l'analyse et du jugement étant donné que ses retombées sur la réduction des risques ne sont pas sûres mais elles peuvent être rentables.

L'*Écart de sécurité*[6] survient lorsque les politiques de contrôle ne sont pas exécutés telles qu'elles sont définies au départ. En effet, les pratiques de sécurité utilisées sont parfois différentes de ce qu'énoncent les politiques. Ces pratiques sont diverses telles que par exemple la divulgation de mots de passe, l'utilisation de disquettes de l'extérieur sans vérifier l'existence de virus, la non déclaration de la détection d'intrusions, etc.

Afin de réussir la politique de gestion du risque inhérent aux projets d'informatisation, certains préalables doivent être bien assimilés par les dirigeants de l'organisation ainsi que l'équipe de projet. Il s'agit d'éléments critiques à surveiller durant la gestion du risque. Dans la section qui suit, nous mettons la lumière sur ces principaux éléments.

---

[3] « Control weakness »
[4] « Possible level of Control risk »
[5] « Control weakness or Control risk-Not clear »
[6] « Security Gap »

2.3 Les facteurs clefs de succès de la gestion du risque

Comme nous l'avons avancé au début de la section précédente, Jones (1994) préconise la nécessité de la présence de certains éléments préalablement à la mise en application d'une politique de gestion du risque efficace. Ces éléments se rapportent principalement au soutien de la direction. D'autres auteurs ont contribué également en avançant d'autres facteurs que nous présenterons dans les sous-sections qui suivent. Ces facteurs se rattachent au soutien de la direction, au choix de la technologie et au facteur humain.

2.3.1 Le soutien de la direction

Jones (1994) prévient de certaines erreurs à éviter durant la gestion du risque et qui sont les suivantes :

1. La mal compréhension des retombées positives de la gestion du risque : souvent, les commanditaires ou même les clients du projet demandent des résultats positifs sans s'attarder au mécanisme de réalisation de ces résultats. Lanza (2001) pense que le gestionnaire ainsi que son équipe de projet sont parfois contraints d'accepter de hauts niveaux de risques sans avoir les moyens requis pour leur gestion.

2. La planification inappropriée de la gestion du risque : la gestion du risque ne doit pas être perçue comme étrangère au processus de planification du projet. Au contraire, elle doit faire partie intégrante du cycle de vie du projet (Lanza, 2001). Idéalement, la gestion du risque doit être entreprise dès le lancement du projet. En effet, il est moins dispendieux de prévenir ces risques dès leur émergence que de les gérer une fois sont devenus éminents (Choo, 2001).

Selon Buttrick (2002), il importe pour la direction d'opter pour un mode de gestion qui puisse favoriser le changement dans l'organisation et l'instauration d'un climat de confiance et de collaboration au sein de l'équipe de projet. La présence d'un tel soutien de la part de la direction pour le projet est de nature à assurer un niveau acceptable de rentabilité et à gérer ainsi le risque

financier. Également, la bonne collaboration de la part de la direction permet à l'équipe de projet d'obtenir le financement nécessaire pour le projet d'informatisation. Ainsi, l'organisation serait en mesure de faire face aux risques de dépassement du budget et de respecter les délais alloués au projet.

Par ailleurs, le soutien qu'elle accorde à lui seul, ne permet pas à la direction d'espérer des résultats positifs si le choix de la technologie n'est pas approprié dans la mesure où il ne répondrait pas à ses orientations stratégiques et ne s'adapterait pas à ses processus d'affaires. Dans la section suivante, nous mettrons la lumière sur les apports de plusieurs auteurs en ce qui concerne l'importance du bon choix de la technologie ainsi que les critères de choix appropriés.

2.3.2 Les critères de choix de la technologie

Les technologies de l'information sont censées améliorer le fonctionnement et la profitabilité de l'entreprise. En effet, les technologies d'information offrent des outils rentables facilitant l'atteinte des objectifs organisationnels à savoir principalement la réalisation de profits. Il importe d'effectuer premièrement une étude sur la rentabilité du nouveau projet avant de procéder à son exécution. Deuxièmement, l'entreprise doit choisir la technologie qui s'ajuste le plus à ses orientations stratégiques.

2.3.2.1 L'étude de rentabilité financière

Une telle étude est de nature à prévenir les problèmes d'ordre financier dès le début et à orienter ainsi le choix de la technologie à implanter. Selon Mantel et Meredith (2000), l'analyse du risque financier consiste essentiellement à utiliser certains indicateurs financiers dans le but d'évaluer la rentabilité du projet. Dans cette perspective, des distributions de probabilité sont utilisées dans l'estimation de certaines variables afin d'évaluer la rentabilité du projet. L'indicateur de la valeur actuelle nette (VAN) représente l'outil privilégié dans l'évaluation de la rentabilité des fonds investis.

Durant l'étude de rentabilité, les chefs de projet doivent prendre en considération l'ensemble des paramètres importants qui entrent en jeu, à savoir le montant de l'investissement initial, les moyens de financement, les flux financiers induits par le projet, les taux d'intérêt sur le marché monétaire, etc. En effet, pour Pradels (1981), il s'agit d'une étude de faisabilité financière dont l'importance se situe à deux niveaux : établir des estimations préliminaires des coûts d'investissement à engager et déterminer les profits escomptés. Ces données une fois établies, peuvent être confrontées aux réalisations après la mise en place de la TI. Sur un autre plan, cette procédure est nécessaire pour l'établissement du budget qu'il convient de respecter durant l'exécution du projet.

Mais trop souvent, les prévisions en matière de dépenses relatives au projet d'informatisation s'avèrent éloignées de la réalité. Cela est dû au fait que certaines rubriques de dépenses ne sont pas prises en considération lors de la prévision initiales. Qui plus est, ces nouvelles rubriques apparaissent à la suite de modifications introduites en cours de route (ARETE, 1986)[7]. En effet, la détermination des coûts doit être bien élaborée. Afin d'aboutir à cette finalité, Mantel et Meredith (2000) pensent qu'il serait préférable de consulter la liste des activités et des tâches relatives au projet dans l'objectif de constater leurs coûts respectifs. Seuls les coûts engendrés par le projet seront pris en considération. Il s'agit de prendre en compte les variations de coût qui sont dus à la seule introduction de la technologie. Les responsables peuvent avoir recours pour cette fin aux dossiers comptables de l'entreprise qui représentent la source d'information la plus riche et la plus fiable.

Par ailleurs, les coûts estimés doivent être assimilés par rapport aux avantages espérés à travers le projet d'informatisation. Ces derniers ne sont pas faciles à estimer mais ils portent généralement sur des données quantitatives telles que par exemple les économies de coût, les gains financiers résultant d'une meilleure gestion de la trésorerie, la réduction des frais de stockage, etc. D'autres avantages sont plutôt d'ordre qualitatif et sont par conséquent difficiles à

[7]Association pour la recherche sur l'emploi des techniques (1986). Réussir l'informatisation de la PME. Paris : Les éditions d'organisation.

évaluer tels que la qualité du service rendu à la clientèle, l'amélioration des délais de livraison, le meilleur accès à l'information, etc. (ARETE, 1986).

Une évaluation exhaustive des coûts et des gains est indispensable quant à l'obtention d'un financement externe pour le projet d'informatisation. En effet, « c'est à partir de sa connaissance des coûts et des gains du projet que l'entreprise peut bâtir, avec l'aide de sa ou de ses banques, un plan de financement réaliste.» (ARETE, 1986). Plus encore, la détermination des différentes catégories et rubriques de coûts permet de sensibiliser l'équipe de projet. En effet, les membres de l'équipe deviennent plus conscients de l'enjeu consistant à comprimer ces coûts et à éviter les dépenses inutiles.

Cependant, l'étude de rentabilité à elle seule ne peut constituer un gage pour la réussite du projet. Il importe de choisir une technologie qui répond le mieux possible aux orientations stratégiques de l'organisation, et ce, pour qu'il n'y ait pas de divergences par la suite entre la technologie implantée et les processus d'affaires déjà mis en place.

2.3.2.2 L'ajustement de la technologie à la stratégie de la firme

Afin de rentabiliser davantage la technologie qu'elle se veut implanter, l'entreprise doit bien définir sa planification stratégique qui englobe sa mission ou sa vocation, sa culture, ses valeurs, ses objectifs et sa stratégie sur le marché (Paquin, 1990). La planification stratégique est une façon d'analyser et de maîtriser les enjeux de la compétition. Elle est un processus de réflexion qui permet à l'entreprise de se doter d'une vision et d'une direction stratégique. Dans ce cadre, les organisations disposent d'un certain nombre de technologies d'information pour « connaître leur état, coordonner leurs processus ou planifier leurs décisions » (Chokron, 1996).

Dans le but d'être à l'avant-garde sur le plan technologique, l'entreprise doit opter pour la technologie qui va de pair avec son plan stratégique et qui lui assure un avantage concurrentiel[8] sur le marché qu'elle vise.

---

[8] L'avantage concurrentiel est un concept fondateur de la pensée stratégique contemporaine. Ce concept consiste dans la détention et la conservation d'un avantage dans un contexte de plus en plus compétitif. Dans ce cadre, trois

Du fait de ce rôle majeur dans l'obtention d'un avantage concurrentiel, il faut également considérer l'évolution de la technologie. Une firme peut prendre les initiatives adéquates et donc s'approprier ou renforcer un avantage concurrentiel en anticipant les avancements technologiques. Une entreprise peut survivre et réussir à long terme si elle élabore les stratégies susceptibles de lui permettre de surmonter les cinq forces concurrentielles auxquelles elle fait face dans son activité, à savoir (1) la rivalité entre les concurrents au sein d'une industrie, (2) la menace des nouveaux venus, (3) la menace des produits de substitution, (4) le pouvoir de négociation des clients et (5) le pouvoir de négociation des fournisseurs (Porter, 1980 ; O'Brien, 1995). Selon Porter (2001), la structure d'une industrie repose sur ces cinq forces qui déterminent l'état de la concurrence et la rentabilité de la concurrence.

Le choix de la technologie est important. Il soutient les efforts de l'entreprise dans la gestion de l'ensemble des cinq forces concurrentielles (Paquin, 1990 et Porter, 2001) :

1. **La rivalité entre les concurrents au sein d'une industrie :** Porter (2001) pense que l'adoption de la technologie, notamment l'Internet, multiplie le nombre des concurrents du fait qu'elle permet à l'entreprise d'avoir accès à plus de parts de marchés. Par ailleurs, Porter (2001) continue en précisant que le recours à l'Internet rend plus intense la concurrence au niveau des prix puisqu'il y aura moins de différences au niveau de l'offre. De plus, les entreprises du secteur sont amenées à supporter plus de coûts fixes. En effet, Paquin (1990) évoque dans ce cadre l'exemple du secteur de la distribution en France où l'automatisation des commandes et de la procédure de facturation a entraîné une hausse des frais fixes des entreprises opérant dans le secteur, ce qui a augmenté la rivalité entre elles.

2. **La menace des nouveaux venus :** certaines technologies ont pour effet d'anéantir les barrières à l'entrée au secteur d'activité visé par l'entreprise surtout si elles sont faciles à

grandes options s'offrent aux dirigeants: atteindre les coûts les plus bas à qualité comparable, offrir un produit unique à coût équivalent ou se concentrer sur un segment-cible. C'est ce que l'on a appelé par la suite «Les stratégies génériques» Porter (1980).

acquérir (Paquin, 1990 et Porter, 2001). Nous évoquons dans ce cadre l'exemple des entreprises virtuelles qui commercialisent des produits en ligne. De telles entreprises, et en s'appuyant sur la technologie Internet, sont venues concurrencer les autres canaux de distribution traditionnels (Porter, 2001).

3. **La menace des produits de substitution :** l'avancement technologique et ses effets quant la réduction des coûts opérationnels offrent des opportunités à saisir pour l'entreprise qui se veut élargir ses parts de marché. En effet, les TI permettent d'innover au niveau des produits de substitution. En effet, en s'appuyant sur des technologies bien développées, il est plus facile actuellement de créer toutes sortes de produits qui se distinguent dans des détails très infimes (exemple : les PC et les ordinateurs portables).

4. **Le pouvoir de négociation des clients :** Selon Paquin (1990), la technologie intervient en dotant l'entreprise des moyens nécessaires qui lui permettront de fidéliser ses clients (agir sur la qualité du produit ou du service offert) et de leur réduire ainsi leur pouvoir de négociation. En ayant recours aux technologies avancées, il est possible pour certaines entreprises de développer certaines caractéristiques clefs dans les produits qu'elles offrent sur le marché. Ainsi, ces caractéristiques seront exclusives à l'entreprise qui déploie une telle approche. Par conséquent, les clients ne trouveront pas ces caractéristiques ailleurs. Cela permet de fidéliser davantage les clients et de réduire leur pouvoir de négociation. Par contre, Porter (2001) pense que l'adoption des technologies, en particulier Internet, permet aux consommateurs de diminuer les coûts de transfert d'un produit à un autre (frais de déplacement nuls), et leur donne en conséquence plus de pouvoir de négociation.

5. **Le pouvoir de négociation des fournisseurs :** en se dotant d'une technologie avancée qui lui permet de comparer rapidement les cotations de plusieurs fournisseurs, l'entreprise est en mesure de réduire le pouvoir de négociation de ses fournisseurs. En effet, l'Internet permet aux entreprises d'aujourd'hui d'avoir accès à toutes les offres émanant de fournisseurs de partout dans le monde. Par conséquent, il est possible de choisir l'offre la plus avantageuse sans avoir une dépendance à l'égard des fournisseurs locaux (Paquin, 1990 et Porter, 2001).

Également, la technologie a une influence directe sur les coûts ou la différenciation des produits. Elle procure ainsi un avantage concurrentiel en réduisant les coûts et en permettant la différenciation au niveau des caractéristiques des produits offerts. Il convient donc de privilégier les technologies qui ont les effets les plus durables sur les coûts ou sur la différenciation. Toutefois, un tel choix ne requiert pas la sophistication prononcée des produits (Paquin, 1990).

Sur un autre plan, Laudon et Laudon (2000) supposent que l'ajustement de la TI adoptée aux orientations stratégiques de l'organisation est de nature à prévenir les risques techniques, de coûts et d'échéancier. En effet, si la TI est conforme aux orientations stratégiques de la firme, elle correspondrait nécessairement aux systèmes légués liés aux processus d'affaires stratégiques. Ainsi, il y aura moins de problèmes techniques, ce qui va réduire les risques liés au dépassement de budget et au dépassement des délais durant la réalisation du projet.

Toutefois, pour que la technologie implantée puisse soutenir la stratégie de la firme, il faut que les employés soient engagés et assez motivés. Il revient ainsi à la direction de bien assigner les tâches aux ressources appropriées, ce qui interpelle la notion de gestion de la structure d'organisation du projet.

2.3.3 La gestion de la structure d'organisation du projet

Le projet apporte certains changements dans la structure de l'organisation étant donné que deux structures seront appelées à coexister, à savoir la structure fonctionnelle et la structure du projet. Cela est de nature à susciter certains conflits au sein de l'organisation tels que principalement le conflit de tâches entre les employés et le conflit de directives émanant des supérieurs fonctionnels et du chef de projet (Buttrick, 2002). Plus encore, Buttrick (2002) prévient du fait que les employés ont parfois de la misère à accepter ces nouvelles structures entraînées par la réalisation du projet. En effet, il avance que « le plus souvent, on affecte au projet des personnes venant de fonctions et de lieux différents », ce qui peut entraîner des conflits au niveau des méthodes de travail entre les participants au projet.

Marchewka (2003) préconise que la structure de n'importe quelle organisation doit correspondre à sa stratégie. Ainsi, l'attribution de la structure d'organisation de l'entreprise aux différents projets qu'elle entreprend permet de contrer les différentes catégories de risques. Évidemment, une organisation peut suivre plusieurs stratégies en même temps, ce qui implique l'adoption de structures différentes. Au fur et à mesure que l'organisation excelle et se développe, elle commence à définir une stratégie et une structure unique et optimale susceptible de soutenir la rentabilité de la technologie adoptée et de respecter le budget et le calendrier fixés.

Dans ce sens, les projets demandent des ressources, des processus et une structure. Marchewka (2003) continue en précisant que la planification de la structure du projet à comme objectif de définir les rôles et de déterminer les responsabilités des individus faisant partie du projet ainsi que les intervenants externes. Il est alors important de choisir les éléments les plus compétents et les plus valables pour le développement de la TI.

Cependant, les éléments clefs que nous venons d'expliciter concernant les facteurs clefs de succès de la gestion du risque des projets de développement de TI au sein des organisations, ne peuvent à eux seuls garantir le succès du projet. Plusieurs auteurs pensent qu'il importe de définir un processus standard de gestion du risque lors de d'implantation des technologies d'information. Un tel processus doit être de nature à prévoir et à limiter les risques potentiels.

Dans ce qui suit, nous présenterons le processus de gestion du risque avancé par Marchewka (2003) qui regroupe un ensemble d'activités à exécuter dans le but de limiter la portée des risques. Dans ce cadre, nous avons eu recours dans notre travail de recherche au modèle avancé par ce dernier étant donné qu'il s'agit d'un processus qui tient compte de l'ensemble des recherches qui ont été faites par d'autres auteurs dans le cadre de la gestion du risque. En effet, l'industrie informatique, et comme nous l'avons déjà mis en relief dans l'introduction, connaît un essor phénoménal ainsi qu'une forte croissance durant les dernières années. Ainsi, il nous incombe de prendre en considération dans le présent travail le processus qui soit le plus à jour. De plus, nous avons pu constater la clarté des éléments qui composent le processus tel que défini par Marchewka (2003), ce qui est de nature à faciliter leur observation lors de la partie empirique.

2.4 Processus de gestion du risque relatif aux technologies d'information

Pour Marchewka (2003), le risque provient de l'incertitude. L'incertitude provient quant à elle de la tendance des gens à prédire le futur sur la base des estimations, des hypothèses et des informations disponibles.

Il est essentiel de bien comprendre la nature des risques et la façon par laquelle ces risques interagissent et influent les autres aspects du projet durant son cycle de vie. Dans ce cadre, le PMBOK (2000)[9] définit la gestion du risque de projet comme étant « un processus systématique d'identification, d'analyse et de réponse aux risques du projet. »

Outre la prévention des risques, la gestion du risque inclut également la maximisation de la probabilité et l'optimisation des conséquences des événements positifs (Buttrick, 2002). La définition du PMBOK (2000) citée dans (Marchewka, 2003) suppose la nécessité de l'existence d'un processus systématique pour gérer efficacement le risque de projet.

Selon Jones (1994), la non utilisation d'un processus standard dans la gestion du risque peut causer une perte de temps et de ressources dans l'analyse et la prévision des problèmes éventuels pouvant survenir. Également, Lanza (2001) attire l'attention des preneurs de décision dans les organisations quant aux opportunités qui pourraient ne pas être saisies en raison de l'ignorance de la situation et du contexte du projet. « L'occurrence des mauvaises surprises se fait sans préavis » (Choo, 2001 : 7). Cela pourrait affecter le moral et la productivité de l'équipe de projet.

Le processus que propose Marchewka (2003) comporte différentes facettes relatives à la gestion du risque des projets d'informatisation que nous présentons dans les prochaines sections. Dans ce sens, nous avons élaboré une illustration graphique de ce processus comportant l'ensemble des éléments de chaque phase du processus (voir la figure 2 dans la page suivante).

---

[9] Project Management Institute. 2000. Project Management Body of Knowledge. http://pmi.org/prod/groups/public/documents/info/PP_CompletedProjectsPMBOK2000.asp

Dans sa première phase, le processus se veut comme finalité la planification des risques. Dans la deuxième phase, il y a lieu de procéder à l'identification des risques du fait que certaines organisations se trouvent actuellement dans des situations de crises perpétuelles à cause de leur mauvaise prévision des risques (Jones, 1994). La troisième phase est consacrée à l'analyse et l'évaluation de l'impact des risques identifiés. Quant à quatrième phase du processus, elle en représente l'étape clef et la plus importante étant donné qu'elle traitera les stratégies et les outils destinés à contrer les risques inhérents au développement de la technologie. Lors la présentation de cette phase, nous aurons recours aux apports de plusieurs auteurs en ce qui a trait à la question des outils de gestion du risque. Enfin, la dernière phase portera sur la surveillance et la réponse aux risques. Marchewka (2003) ainsi que d'autres auteurs que nous verrons consacrent cette phase à la réévaluation de l'ensemble du processus et de son efficacité.

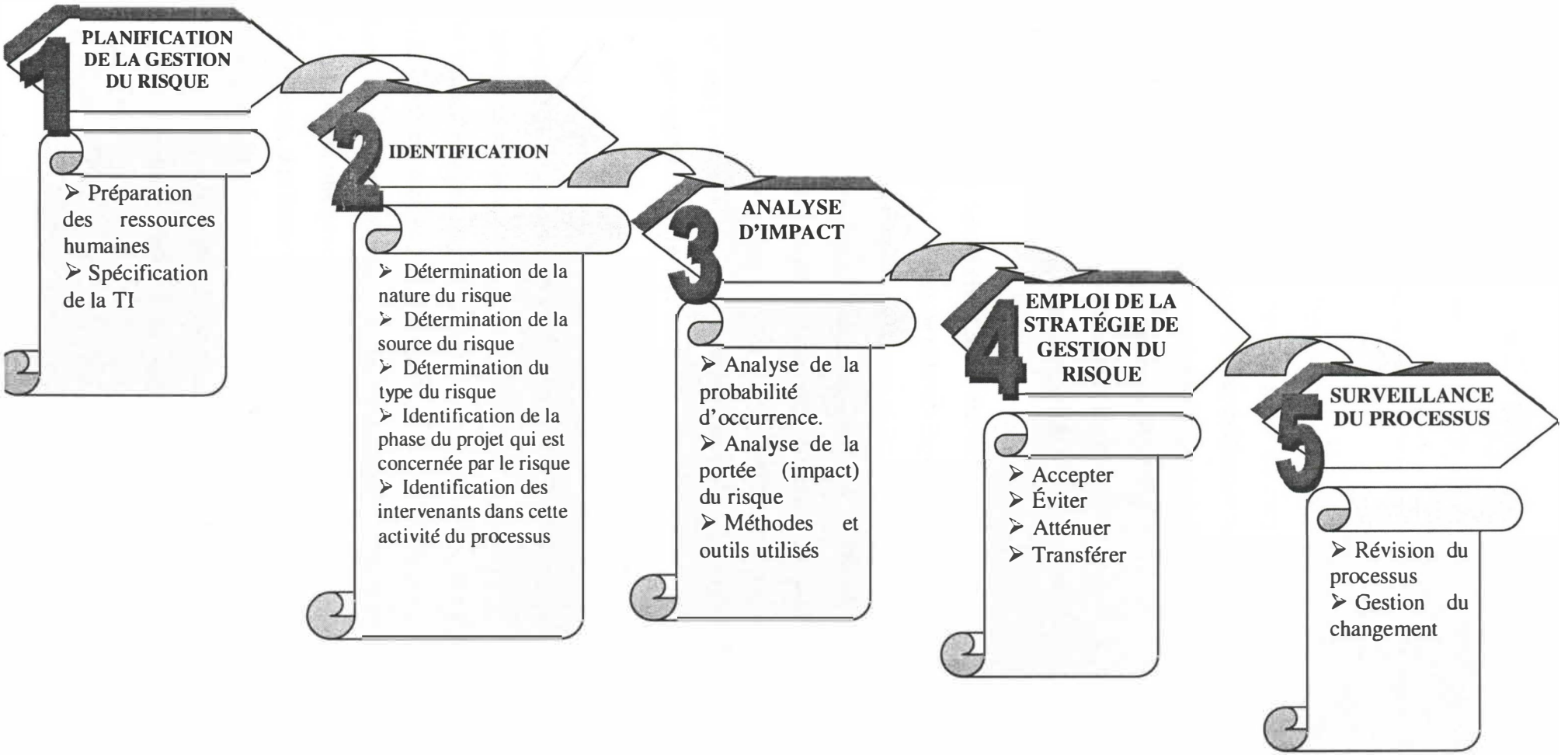


Figure 2 : Illustration graphique du processus de gestion du risque associé à l'implantation des technologies d'information (adapté de Marchewka, 2003).

2.4.1 La planification du risque

Il s'agit de s'assurer de l'engagement de toutes les parties impliquées dans le projet, dans la mesure où cela permet de mettre en place les moyens appropriés pour prévenir et gérer les risques. Ces moyens se rapportent essentiellement aux ressources humaines, au temps et à la technologie. Une bonne préparation est de nature à limiter les effets adverses et à permettre de saisir les opportunités au bon moment. Pour Barki, Talbot et Rivard (1993) ; Greenstein et Vasarhelyi (2002) et Barki, Bourdeau et Rivard (2003), le facteur humain représente le facteur le plus difficile à gérer dans le cadre des projets d'informatisation.

Greenstein et Vasarhelyi (2002) énumèrent certains risques inhérents au facteur humain dont principalement les risques de mauvais jugement, d'erreurs, de fraudes et de virus. Il s'agit de bien mettre en exécution les politiques et les mesures appropriées et de les communiquer aux employés. Certaines firmes demandent à leurs employés de signer des déclarations dans lesquelles ils attestent de leur pleine compréhension des politiques et de leur engagement à les appliquer convenablement. Barnes (2001) préconise que les attentes des employés et des utilisateurs potentiels doivent être prises en considération dès le début afin d'éviter la réalisation des risques inhérents au facteur humain.

Sur un autre plan, Feringa, Goguen et Stonebumer (2001) dédient la phase de planification du risque à la caractérisation de la technologie à implanter, et ce d'un point de vue ressources requises et contenu informationnel. Concernant les ressources, il importe de préciser le matériel et les applications requis pour le développement de la technologie. De plus, il faut déterminer les interfaces du système et les personnes qui auront à intervenir durant le projet et ceux qui vont utiliser la technologie par la suite. Sur un autre plan, Feringa et al. (2001) continuent en précisant que les informations portant sur le contenu de la technologie, peuvent être puisées à partir des questionnaires, des interviews et la revue de la documentation. D'ailleurs, McLaughlin (2003) affirme que de telles techniques doivent apporter des éclaircissements quant à l'organisation du travail entre les différents départements ainsi que les informations sollicitées par ces derniers dans leur fonctionnement. Une fois la planification de la gestion du risque effectuée,

l'organisation sera en mesure de procéder à l'étape clef du processus, à savoir l'identification des risques.

2.4.2 L'identification des risques

L'identification des risques comprend la détermination des menaces et des opportunités pouvant avoir un effet sur l'aboutissement à l'objectif final du projet (Buttrick, 2002 ; Marchewka, 2003). Comme nous venions de le voir dans la section précédente, Feringa et al. (2001) recommandent de procéder au préalable à l'étude et à la documentation des caractéristiques de la technologie à développer afin de fournir une base pour le reste du processus de gestion du risque. Il est cependant important de bien cerner l'ensemble de ces risques en ayant une vision minutieuse du projet et de l'ensemble de ses composantes. Ainsi dans la sous-section suivante, nous approfondissons la classification des risques relatifs aux projets d'informatisation. Sur un autre plan, la deuxième sous-section présentera les risques inhérents a la technologie Internet et ses dérivées.

2.4.2.1 La classification des risques

Marchewka (2003) propose un cadre d'analyse pertinent quant à l'identification des risques et de leur source de provenance (voir la figure 3).

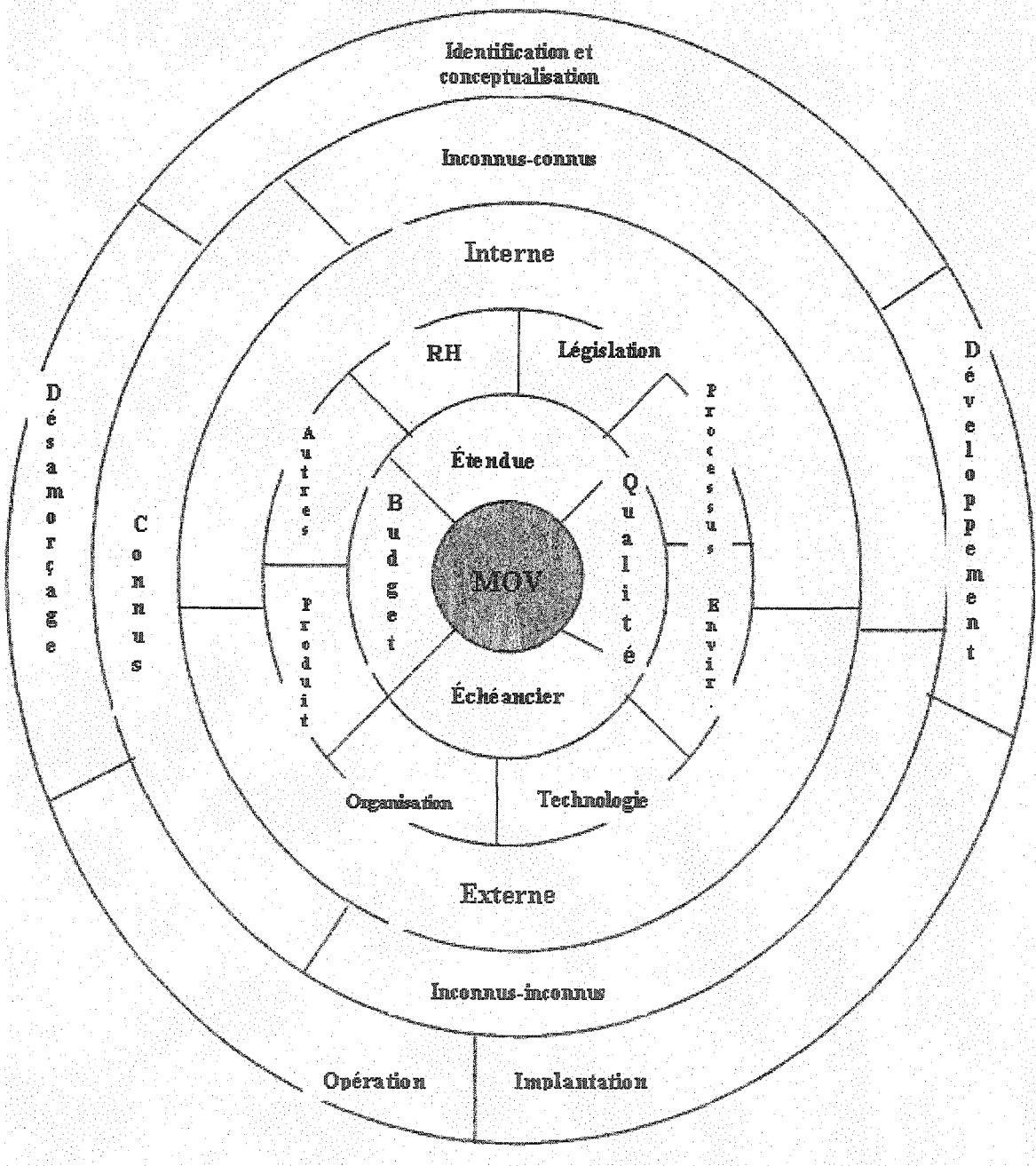


Figure 3 : Cadre conceptuel de la gestion du risque des TI (adapté de Marchewka, 2003 :)

1) La **valeur de l'entreprise** (MOV[10]) est mise au centre du graphique. La MOV représente le but du projet consistant à générer de la valeur pour l'organisation. Cette valeur représente à la fois une définition et une mesure du succès du projet. Barnes (2001) pense que l'importance des coûts associés à l'implantation de la technologie deviendrait négligeable si cette dernière était génératrice de valeur pour l'organisation.
2) La deuxième couche du graphique représente les **objectifs du projet** en termes d'envergure, de budget, de qualité et d'échéancier. Ces objectifs doivent être appréhendés comme un tout pour pouvoir se renseigner sur le succès du projet. Ils soutiennent ainsi la valeur de l'entreprise. De plus, il importe selon Ward (2003) d'établir au départ des mesures de succès aussi bien quantitatifs que qualitatifs dans le but de renseigner sur la performance de la technologie à implanter.
3) La troisième couche met la lumière sur les **sources potentielles des risques**. Les risques peuvent provenir des personnes participantes au projet, de certaines dispositions légales, des processus (projet et produit), de l'environnement, de la technologie, de l'organisation ou du produit. Greenstein et Vasarhelyi (2002) avancent que le facteur humain représente la première source de risques durant l'implantation des technologies d'information dans l'entreprise.
4) La couche suivante met l'accent sur la **nature du risque** que ce soit interne ou externe au projet. Cette distinction est importante dans la mesure où le gestionnaire du projet serait responsable de la réalisation de n'importe quel risque interne. Néanmoins, une telle distinction n'est pas toujours facile à établir du fait que le gestionnaire de projet ne peut ignorer les risques externes. Plus encore, et comme nous l'avions explicité dans le chapitre précédent, les risques peuvent être catégorisés en risques de rentabilité, de technique, de coût ou d'échéancier.
5) La cinquième couche dissocie entre trois **types de risques** : connus, connus-inconnus, et inconnus-inconnus. Les risques connus sont ceux qui vont survenir avec certitude (Wideman, 1992). Quant aux risques connus-inconnus, l'incertitude en caractérise une partie. Par exemple, on est parfois sûr de la réalisation du risque mais on ne connaît pas

[10] MOV : Measurable Organizational Value

l'amplitude de son impact. Par ailleurs, l'incertitude et l'imprévisibilité portent sur la totalité des risques inconnus-inconnus.

6) La dernière couche renseigne sur les différentes **phases du cycle de vie du projet.** Cette délimitation temporelle s'explique par la nécessité d'offrir aux responsables du projet la possibilité de bien situer temporellement les risques inhérents à leur projet (Quand cela peut-il arriver ?). Cela met l'accent également sur la nécessité de la vigilance aux opportunités tout au long du développement du projet. Selon Feringa et al. (2001), la gestion du risque est une méthodologie pouvant être entreprise au niveau de chaque phase du projet de développement des technologies d'information. Ils continuent en précisant la façon par laquelle la théorie de gestion du risque intervient lors du cycle de vie de la TI. Ils présentent cinq phases, à savoir :

Phase 1 : Identification et conceptualisation

Durant cette phase, il y a lieu de procéder à l'identification des besoins pour la technologie d'information désirée ainsi qu'à la définition de son envergure. La gestion du risque intervient lors de cette phase dans le but d'aider les décideurs à déterminer les attributs essentiels de la technologie d'un point de vue sécurité et fonctionnement.

Phase 2 : Développement ou acquisition

Au niveau de cette phase, la technologie d'information est destinée à être conçue, achetée, programmée et développée. Les risques identifiés durant cette phase permettront d'introduire les changements et les rectifications nécessaires à la technologie.

Phase 3 : Implantation

Les paramètres de sécurité de la technologie d'information doivent être configurés, appliqués, testés et vérifiés. La gestion du risque permet de vérifier la correspondance entre les réalisations relatives à la technologie d'information implantée et les prévisions.

Phase 4 : Opération et maintenance

Les fonctions de la TI sont opérationnelles au niveau de cette phase. La technologie d'information implantée est appelée à subir des modifications selon les

politiques organisationnelles constamment changeantes. Dans ce cadre, la gestion du risque permet de réévaluer l'utilité de la technologie mise en place suite aux modifications introduites.

Phase 5 : Désamorçage

Il s'agit de la suppression de certains matériels ou applications relatifs à la technologie implantée. La gestion du risque permet de s'assurer de l'intégrité des informations gérées par la technologie ainsi que du succès ou non de la migration vers d'autres systèmes.

La figure 3 est importante pour notre travail de recherche dans la mesure où elle permet de pousser davantage l'identification des risques. En effet, nous venons de voir dans la section 2.1 les quatre catégories majeures des risques pouvant rencontrer les projets d'informatisation, à savoir le risque financier, technique, de coût et d'échéancier. Suite à cette première phase d'identification, il importe de procéder à la deuxième phase que nous venons de voir dans le cadre du graphique 3 et qui permet d'établir des distinctions au niveau des risques, et ce, par rapport à leurs sources, à leur nature, à leur type et également par rapport à la phase du cycle de vie du projet dans laquelle ils interviennent. Nous notons par ailleurs que cette deuxième phase d'identification intervient lors de l'étape 2 du processus de gestion du risque (figure 2).

Marchewka (2003) explique qu'il a conçu ce modèle dans l'objectif d'aider l'organisation à agir de façon proactive face aux risques. En effet, Marchewka (2003) fait remarquer que la plupart des organisations adoptent souvent une position réactive après que les risques soient déjà devenus des problèmes. Parfois, les responsables du projet ont tendance à camoufler certains risques par crainte d'être accusés de manque de compétence.

Néanmoins, il importe de détecter les différentes corrélations pouvant exister entre ces risques. Ainsi, l'équipe de projet serait en mesure d'étudier l'impact qu'auront ces risques sur le déroulement du projet. Il s'agit de se pencher sur les objectifs pouvant être interrompus par la réalisation potentielle de ces risques. La structure de fractionnement du travail ou la *Work Breakdown Structure* (WBS) fournit un appui considérable dans l'identification des risques.

Cependant, Marchewka (2003) affirme qu'il existe une certaine relativité dans l'appréhension des risques. En effet, un risque qui paraît négligeable pour quelqu'un, peut être un danger urgent pour d'autres. Par conséquent, il est possible que les dirigeants centrent leur attention principalement sur un risque bien déterminé (qui peut également ne pas se réaliser), au détriment du reste des risques. Afin de pallier à ces éventualités indésirables, il est recommandé de laisser l'initiative au gestionnaire du projet et à son équipe dans l'identification des risques et de leur portée. Pour Buttrick (2002), l'équipe de projet serait la première responsable de l'identification des risques inhérents au projet. Toutefois, Fitcher (1999) et McLaughlin (2003) rappellent la nécessité d'impliquer tous les utilisateurs potentiels de la technologie dans l'identification des risques.

Sur un autre plan, l'auteur du modèle fait avancer certaines techniques d'identification des risques. Il propose la technique de « Check-list » qui consiste dans le recensement des risques déjà rencontrés dans le cadre d'autres projets précédemment entrepris. Ensuite, l'équipe de projet serait en mesure d'apprendre des erreurs du passé. Également, certaines organisations ont recours aux diagrammes de cause à effet pour faire apparaître les risques, leurs causes ainsi que leurs effets.

Dans la section suivante, nous tenterons d'introduire le contexte de ce travail de recherche en présentant les principaux risques inhérents aux réseaux de communication interne à l'organisation et basés sur la technologie Internet, à savoir les Intranets et les Extranets. Sur un autre plan, nous proposerons les techniques et les méthodes visant la réduction de ces risques. Par la suite, le dernier chapitre sera consacré à l'étude de la façon par laquelle le processus de gestion du risque est appliqué au sein de certaines firmes québécoises, et ce, à travers une série d'études de cas basées sur des entrevues en profondeurs avec les dirigeants et les concepteurs des réseaux basés sur Internet.

2.4.2.2 Les risques relatifs aux réseaux de communication basés sur Internet

Dans le cadre des objectifs de notre travail de recherche, nous traiterons la technologie Internet y compris ses dérivées, à savoir l'Intranet et l'Extranet. Il s'agit de réseaux de communication internes à l'entreprise qui ont connu de l'essor durant ces dernières années en raison de la convenance, la rapidité et les coûts relativement faibles qui leur sont associés. En effet, dans ses débuts, l'Internet offrait aux employés des informations statiques. Actuellement, les firmes gèrent de plus en plus leurs affaires critiques via cette technologie révolutionnaire. Les utilisations fréquentes de la technologie Internet se rapportent à la circulation et le partage de l'information, les courriels et la gestion de la documentation (Henry, 1999). Laudon et Laudon (2000) situent les apports des réseaux de communication interne basés sur Internet pour les organisations sur quatre niveaux à savoir : la finance et la comptabilité (rapports et états comptables et financiers, évaluation des projets, établissement des budgets) ; les ressources humaines (politiques de l'entreprise, adhésion des employés aux avantages sociaux, affichage des postes vacants, information, etc.) ; la fabrication et la production (mesures de qualité, spécifications, détails techniques sur les équipements de production, suivi des commandes, etc.) et la vente et le marketing (analyse de la concurrence, mise à jour des prix, promotions, etc.).

Nous proposons dans ce qui suit, et en se basant sur la vision concrète et l'expérience de certains auteurs, certains risques d'ordres financier, technique, de coût ou d'échéancier, relatifs à la technologie Internet au sein des entreprises. Également, nous présenterons des outils ainsi que des approches destinés à gérer l'ensemble de ces risques et à garantir ainsi le succès de l'implantation de cette technologie dans l'organisation. Dans ce cadre, Fitcher (1999) précise qu'il n'existe pas toutefois de « recette à succès » de gestion conçue spécialement pour réussir l'implantation de l'Internet et de ses dérivées. Nous notons dans ce cadre que cette section représente une mise en contexte au présent travail de recherche et qui tentera de voir de près sur le terrain la façon par laquelle certaines firmes québécoises gèrent les risques relatifs aux réseaux de communication internes développés.

2.4.2.2.1 Le risque financier

Karolak (1996) et Laudon et Laudon (2000) avaient évoqué ce type de risque inhérent à tout projet visant le développement de technologie d'information au sein des entreprises. De tels risques demandent d'être bien maîtrisés étant donné qu'ils affectent directement la rentabilité de l'investissement ce qui signifie des pertes importantes pour l'organisation. Ces pertes sont plus importantes surtout lorsqu'il s'agit d'un projet d'envergure. Nous citerons en premier lieu le risque de mauvaise performance qui est associé à n'importe quel projet mené par l'entreprise, ainsi que les moyens visant à garantir un niveau acceptable de rentabilité. En second lieu, nous éluciderons le risque de fraudes de la part des employés de la firme qui sont de nature à réduire la productivité de la technologie d'information adoptée. Enfin, nous traiterons la question de la responsabilisation qui est importante dans la mesure où elle est susceptible de mobiliser l'ensemble des acteurs de l'organisation à réussir et à fructifier la rentabilisation du réseau de communication mis en place.

2.4.2.2.1.1 Risque de mauvaise performance

Dans le cadre du développement de réseaux de communication basés sur la technologie Internet, il est préférable de procéder à l'évaluation de la performance du réseau de communication mis en place (Mantel et Meredith, 2000 et Pradels, 1981). Selon Barnes (2001), la définition des mesures de la rentabilité de la technologie d'information repose sur les objectifs personnels et organisationnels recensés et établis au départ. Ces objectifs sont censés déterminer le contenu du réseau. Les normes traditionnelles telles que le temps de réponse, les hyper-liens entre les pages du site Web, ne peuvent pas renseigner sur l'impact du réseau développé par l'organisation. Dans ce sens, les résultats doivent être relativisés par rapport aux attentes des utilisateurs. Par exemple, si l'objectif est d'offrir un meilleur accès à l'information pour le service à la clientèle, la mesure idéale serait le temps moyen des appels établis. Pour McLaughlin (2003), il importe également de prendre en considération le coût de l'information contenue dans le réseau. Si l'information est génératrice de valeur pour la firme, l'importance relative des coûts sera minimisée durant l'évaluation de rentabilité. Toutefois, McLaughlin (2003) ajoute que dans le cas

où le coût de l'information est élevé, ou encore si cette dernière ne génère pas assez de valeur, il serait plus opportun alors de ne pas inclure cette information dans le réseau.

Ward (2003) préconise que la rentabilité du réseau doit être mesurée par des indicateurs de succès prédéterminés renseignant sur la performance aussi bien quantitative que qualitative de la technologie. Il s'agit de mesurer le retour sur investissement (ROI : Return On Investment), d'enquêtes, de groupes de discussion, de lignes d'assistance, etc. Le ROI devient la mesure la plus sollicitée étant donné l'importance des fonds et des investissements consacrés pour le développement des réseaux de communication basés sur Internet. Dans ce cadre, il importe de prendre en considération les économies de coût induites par l'utilisation de ces réseaux et portant essentiellement sur les frais d'administration et des ressources humaines, la gestion des systèmes d'information, les opérations financières, les opérations techniques, la productivité des employés, etc. Ward (2003) continue en citant l'exemple de la compagnie *Mitre Corporation* qui avait réalisé des économies de coûts relatifs à l'adoption d'Intranet de l'ordre de 62.1 millions de dollars US sur un investissement de 7.2 millions de dollars. D'autres mesures simples sont à prendre en considération telles que le nombre de visites par page, le nombre de visiteurs, le temps moyen des sessions ouvertes par utilisateur, le délai de rotation du contenu sur le site[11], etc.

2.4.2.2.1.2 Risque de fraude

Le risque de fraude peut survenir suite à l'implantation de la technologie. Toutefois, et étant donné les graves conséquences que les fraudes peuvent engendrer, il s'avère important de tenir compte de ce risque durant l'implantation. Dans ce sens, il est éminent de cerner les différentes facettes du risque de fraude pour pouvoir mettre en place les mesures appropriées en vue de le contourner.

Dans le cadre du risque de fraude, il ne fait pas de doute que les attaques qui causent le plus de pertes pour l'entreprise sont celles qui proviennent de l'intérieur. Les utilisateurs internes comme les employés, les anciens employés, les contractants et certains fournisseurs sont

[11] From headlines to archives.

susceptibles d'attaquer les réseaux d'information de l'entreprise, tel que présenté dans le guide publié en 1999 par la compagnie Verisign Inc. concernant la sécurisation des Intranets et des Extranets. Verisign Inc. (1999) cite également l'enquête menée en 1998 par le Computer Security Institute et le FBI auprès de 520 compagnies aux Etats-Unis. Les résultats montrent que 44% d'accès non autorisés proviennent de l'intérieur comparé à 24% d'intrusions externes.

Il est à mentionner en premier lieu les risques de fraudes de la part de certains employés de la firme et qui sont de nature à réduire la rentabilité du réseau de communication implanté (Greenstein et Vasarhelyi, 2002). Selon Marchewka (2003), ces attaques sont menées généralement par des employés ayant un niveau hiérarchique inférieur dans l'organisation. L'auteur préconise qu'il s'agit des personnes les plus susceptibles d'attaquer les réseaux existants en raison de leur mécontentement de leur situation actuelle. Par conséquent, les mesures de contrôle devront être plus accentuées à ces échelons de l'organisation.

Néanmoins, Marchewka (2003) démontre que le risque de fraude peut provenir également des niveaux supérieurs de la hiérarchie. En effet, les dirigeants de la firme ont le privilège d'avoir un accès facile à toutes les données ainsi qu'à tous les mots de passes utilisés par les employés. Marchewka (2003) prévient que certains parmi ces hauts dirigeants peuvent se permettre parfois de passer outre les mesures de contrôle relatives aux réseaux de communication de l'entreprise en abusant du pouvoir que leur procure le poste qu'ils occupent. Ce risque est d'autant plus important lorsque la position du sujet est haute dans la hiérarchie de l'organisation. Les mécanismes internes de contrôle deviennent sans valeur lorsqu'ils ne sont pas respectés par les dirigeants. Plus encore, ces derniers devraient présenter des exemples à suivre par l'ensemble des employés.

Le contournement des mesures de contrôle peut être mené souvent dans le cadre de fraudes financières de la part de certains employés. Cela renseigne également sur la nécessité d'appliquer les mesures de contrôle à tous les niveaux de l'organisation, sans exception. Marchewka (2003) insiste sur la nécessité de l'engagement d'auditeurs indépendants ainsi que d'experts en matière de réseaux de communication, ce qui permet de garantir l'intégrité du patrimoine informationnel

de l'entreprise. Ces ressources doivent être en mesure de fournir des comptes rendus régulièrement au conseil d'administration.

Pour Greenstein et Vasarhelyi (2002), il s'agit de mettre en exécution les politiques et les mesures appropriées et de les communiquer aux employés. Certaines firmes demandent à leurs employés de signer des déclarations dans lesquelles ils attestent de leur pleine compréhension des politiques et de leur engagement à les appliquer.

Sur un autre plan, certains conflits de pouvoir peuvent causer des problèmes d'ordre financier. Il s'agit en fait du désir de certains dirigeants à garder le pouvoir décisionnel ainsi que le contrôle en refusant d'accorder toutes les informations aux employés à travers la technologie Internet. Dans la sous-section qui suit, nous discutons, en confrontant les apports de plusieurs auteurs, de la question du contrôle et du pouvoir (l'empowerment), et ce, dans le but de trouver la meilleure façon pour optimiser le fonctionnement et la rentabilité de la technologie Internet implantée.

2.4.2.2.1.3 La responsabilisation des employés

Pour Duane et Finnegan (2002), il est évident que les réseaux de communication internes à l'entreprise basés sur Internet, sont susceptibles de développer des compétences au sein de l'organisation. Toutefois, l'expansion de tels réseaux est subordonnée à une gestion équilibrant le souci de contrôle de la direction d'une part et le besoin de délégation d'un certain degré de pouvoir aux employés d'autre part[12].

L'un des avantages les plus révélateurs des réseaux de communication internes basés sur Internet est le pouvoir qu'ils accordent aux différents échelons de l'organisation par le biais de la responsabilisation. La responsabilisation étant un processus par lequel l'entreprise développe un périmètre interne, à l'intérieur duquel elle tolère l'exercice d'un comportement donné et permet

[12] Duane et Finnegan (2002) ont appelé ce phénomène l'« **empowerment** »

aux individus d'expérimenter et de tester leurs connaissances avec une certaine liberté d'action (Fatout, 1995).

Sur un autre plan, certains auteurs comme Damsgaard et Scheepers (1999) pensent qu'il importe de mettre en place des limites à la responsabilisation dans les organisations. En effet, une des raisons poussant à l'adoption de la technologie du Web étant sa grande simplicité d'utilisation et d'implantation. Par ailleurs, et en dépit de ce constat, le manque de contrôle risque de mener à un environnement-système totalement anarchique (Duane et Finnegan, 2002). Fitcher (2003) pense que la technologie Internet développe l'esprit d'autosuffisance – en termes d'informations - auprès des employés. Par conséquent, la question de contrôle représente une interrogation d'envergure souvent soulevée au sein des organisations optant pour la technologie Internet (Ryan, 1997).

Dans cette perspective d'analyse, plusieurs auteurs ont examiné les stratégies ainsi que les tactiques devant être déployées par des organisations en vue de contrôler et de coordonner le développement du Web. Les dirigeants sont appelés à déterminer un dosage optimal de la démarche de responsabilisation tout en préservant un contrôle suffisant sur les informations dans l'organisation (Duane et Finnegan, 2002).

Simons (1995) a défini un modèle pour établir l'équilibre idéal entre la responsabilisation et le contrôle. Ce modèle identifie sept niveaux de contrôle devant être mis en place afin de s'assurer de la bonne utilisation du pouvoir conféré aux employés par la technologie Internet. Le modèle établi par Simons en 1995 et adapté par Nelson et Todd en 1999, consiste en fait en un certain nombre d'activités de management - testées et validées empiriquement - concourant à la définition des sept systèmes de contrôle, à savoir :

1. Le système de croyances : les employés doivent être conscients de la mission principale, des buts et des objectifs de la technologie Internet.
2. Le système de limitation de pouvoir : il s'agit de définir ce que les employés ne sont pas censés faire. Ils sont appelés par conséquent à faire intervenir leur créativité à l'intérieur même de ce champ de pouvoir.

3. La standardisation limitée : la standardisation excessive ne doit pas limiter les opportunités de créativité ou l'efficacité du réseau. Les standards définis dans le contexte d'Internet et les outils qui s'y rattachent doivent représenter un catalyseur pour la créativité. Il s'agit surtout de standardiser le contenu et non pas les outils qui créent le contenu.
4. Le système de diagnostic : la responsabilisation ne sous-entend pas la suspension du contrôle. En l'absence du contrôle sur les inputs ou sur le processus, les employés seront les seuls responsables des outputs ou de la performance finale. Les buts, les objectifs, les standards et les politiques de l'entreprise, servent comme base de référence à toute évaluation de performance.
5. La motivation (les incitatifs) : la responsabilisation implique une plus grande responsabilité, ce qui signifie plus de risques. Les employés-utilisateurs doivent être récompensés et reconnus individuellement pour leurs contributions. Dans ce cadre, les incitatifs peuvent être d'ordre financier ou non.
6. Le contrôle interne : le contrôle interne sous-tend les procédures de vérification et les comptes-rendus dont le but est de préserver les actifs ainsi que l'intégrité des informations.
7. Le système de contrôle interactif : le système de contrôle interactif assure la transmission de l'information et l'apprentissage horizontalement et verticalement dans l'organisation. Par conséquent, ce système de contrôle est de nature à fructifier le savoir, les connaissances et l'expérience de l'employé utilisateur.

Nous avons remarqué tout au long de cette section la multitude de risques financiers auxquels peut faire face tout effort d'introduction d'Internet. En effet, la performance de la technologie doit être observée, étudiée et définie sur la base de certains objectifs avant son implantation. Également, il importe de prévenir le risque d'attaques ou de fraudes de la part de certains intervenants en établissant les mesures de sécurité appropriées. De plus, il est indispensable d'étudier et de prévoir la question de responsabilisation, souvent associée à l'adoption de la technologie Internet, et ce, afin d'éviter tout conflit d'intérêt au sein de l'organisation. Sur un autre plan, les risques techniques en matière de technologie Internet sont très graves à subir, dans la mesure où ils peuvent causer des pertes de matériels et de logiciels coûteux. Il importe alors pour l'organisation d'être consciente de ces risques et de savoir comment les gérer. Dans la section suivante et à travers les expériences concrètes des auteurs, nous présenterons l'ensemble des risques techniques couramment rencontrés dans le cadre des

réseaux de communication basés sur Internet. Nous avancerons également certains outils destinés à la gestion de ces risques.

2.4.2.2.2 Le risque technique

Les ressources informatiques aussi bien logicielles que matérielles font face à des menaces de défaillances (Karolak, 1996 et Waltner, 1999) ou même d'attaques (Marchewka, 2003 ; Verisign, Inc., 1999 et Laudon et Laudon, 2000) susceptibles de causer des problèmes d'ordre technique pour les utilisateurs. En effet, les programmes relatifs aux réseaux peuvent être altérés jusqu'à ce qu'ils deviennent inopérants. Très souvent, les violations des mesures de sécurité sur les réseaux de communication proviennent de personnes internes à l'organisation (Marchewka, 2003).

Le risque de sécurité couru à travers l'utilisation des réseaux se manifeste à travers l'interception de certaines données importantes lors d'échanges entre deux parties sur le réseau. Le problème est que les parties ne conviennent pas au début sur les liens de communication devant être établis (Verisign, Inc., 1999). En effet, l'accroissement de la complexité du réseau a augmenté l'éventualité d'attaques et d'intrusions en provenance aussi bien de l'intérieur que de l'extérieur de l'organisation. Selon l'enquête menée par le FBI, 24% des firmes étudiées disent avoir été dépossédées d'informations très sensibles de la part de cyber-criminels.

Dans l'objectif d'éviter les défaillances techniques associés aux réseaux de communication, Waltner (1999) appelle les concepteurs à bien exploiter l'évolution de la technologie et à maîtriser les nouveaux outils technologiques. En effet, de tels outils entraînent une amélioration significative dans la gestion de la technologie basée sur le Web. Toutefois, certains de ces outils représentent une difficulté d'appréhension considérable et ne sont pas par conséquent faciles à mettre en application. Les compagnies sont appelées à faire de plus en plus recours à ces outils pour pouvoir bien gérer le contenu du site Web au fur et à mesure que le niveau de complexité de ses affaires augmente.

En définitive, Verisign, Inc. (1999) pense que le choix d'un outil dans le but de sécuriser les communications établies entre l'organisation et ses partenaires requiert comme préalables

l'identification des besoins de l'organisation pour un système de sécurité selon la nature et l'objet de ses communications (assurer l'intégrité du contenu et/ou la non répudiation, etc.). L'identification des besoins doit toucher aussi bien le court que le long terme et elle ne doit pas se limiter aux besoins requis par une certaine opération ou dans le cadre d'une affaire avec un partenaire donné.

Les projets de développement de réseaux de communication basés sur Internet peuvent parfois dépasser leur budget et engendrer des coûts difficiles à supporter. Le principal risque de coût consiste dans le conflit qui peut naître entre la distribution en ligne et les canaux de distribution traditionnels. En effet, cela arrive quand deux canaux offrent le même produit, ce qui signifie un gaspillage de ressources. Dans la section qui suit, nous discutons davantage cette catégorie de risque et nous présentons une approche destinée à faire éviter à l'entreprise de gaspiller ses ressources.

2.4.2.2.3 Le risque de coût

Le conflit entre les canaux de distribution représente un risque de coût supplémentaire au projet dans la mesure où l'entreprise sera obligée de réviser la conception de son site Web afin de respecter la vocation de chaque canal de distribution. En effet, chaque canal de distribution doit avoir sa raison d'être afin qu'il soit rentable. L'utilisation des réseaux de communication comme canal de distribution pour l'organisation peut générer un avantage compétitif pour les entreprises qui en font recours du fait qu'il leur permet de faire des économies de coûts importantes (McLaughlin, 2003). En effet, il existe différents canaux de distribution susceptibles d'être utilisés par les firmes dans le but d'écouler leurs produits. Il s'agit principalement des ventes en magasins et succursales, la vente par téléphone et la vente via les réseaux Internet et Extranet.

Toutefois, Aboubekr et Rivard (2002) préconisent qu'en ayant recours à l'Internet ou à l'Extranet pour offrir des produits à des clients particuliers, l'entreprise risque de créer un conflit interne entre ses canaux de distribution. En effet, la problématique qui se pose pour ces entreprises est de déterminer quelle catégorie de produits offrir électroniquement. La résolution de cette problématique est importante dans la mesure où elle permet aux organisations de bien

centrer leurs efforts en évitant de vendre le même produit à des prix distincts selon les canaux de distribution utilisés.

Il importe alors de bien définir les critères de sélection requis du produit en question pour chaque canal de distribution à utiliser. Aboubekr et Rivard (2003) recommandent de distribuer en ligne les produits dont le prix intervient avec force dans le processus d'achat du client. Ce sont généralement des produits peu différenciés. Sur un autre plan, ils avancent que les consommateurs n'ont pas à entrer en « interaction physique » avec les produits distribués en ligne dans le sens où ils sont en mesure de baser leur décision d'achat sur une photo du produit ou même sur son devis technique.

Aboubekr et Rivard (2003) suggèrent aux entreprises de se situer du côté du client lors de son processus d'achat pour tester l'opportunité du choix de l'Extranet comme canal de distribution privilégié. Pour ce faire, ces auteurs dissocient les activités simples des activités complexes composant le processus d'achat du client potentiel. Ils précisent que les activités simples sont celles susceptibles d'être réalisées sans l'aide particulière de la part de professionnels ou d'experts. Par contre, les activités complexes demandent cette aide particulière pour être réalisées. De plus, ils préconisent qu'il est possible et même avantageux d'automatiser les activités simples.

Campbell (1988) attache la complexité d'une activité à des attributs particuliers. Premièrement, il note la présence de plusieurs objectifs reliés à l'activité. En effet, le niveau de complexité de la tâche s'accroît au fur et à mesure qu'il y a plus d'attentes auxquelles il importe d'apporter des réponses. Deuxièmement, Campbell (1988) met l'accent sur la présence de solutions ou de réponses multiples : ceci rend l'activité davantage plus complexe lorsqu'il y a lieu d'interdépendances conflictuelles entre ces différentes options.

À la fin du processus d'achat, Aboubekr et Rivard (2003 : 6) font constater que « le client choisira le canal de distribution qui lui offre de la valeur ajoutée. » La valeur ajoutée d'un canal de distribution consiste en l'aide potentielle qui puisse être fournie au client à mesure que le niveau de complexité de l'activité en question augmente. « La pertinence de l'utilisation de

l'Internet sera évaluée en fonction de son apport en termes de valeur ajoutée pour le client. » Le choix de l'Internet sera abandonné dans le cas où il se révèle que certaines activités du processus d'achat, requerraient de l'interactivité avec un représentant de la vente afin d'éclaircir certains détails et de fournir certaines explications au sujet du produit. Dans la prochaine section, nous tentons de présenter certains risques pouvant engendrer un retard dans l'exécution ou dans l'exploitation de la technologie Internet.

2.4.2.2.4 Le risque relié à l'échéancier

Nous avons expliqué dans la section relative à la théorie de la gestion du risque que la disponibilité des ressources ainsi que l'adhésion des employés aux technologies implantée est de nature à garantir le respect des délais et des jalons établis au départ.

La question qui se pose également est comment réaliser à temps un projet et comment gérer une technologie impliquant des personnes se trouvant en dehors des frontières de l'organisation (Nelson, 1999) ? Il s'agit en fait de la nécessité de bien organiser un nouvel environnement de travail imposé par l'adoption d'Internet. En effet, les réseaux de communication basés sur Internet élargissent les frontières de l'organisation et font intervenir des ressources humaines n'ayant jamais eu affaire ensemble. Cela est de nature à retarder en quelque sorte la fructification des apports bénéfiques de cette technologie. Il implique également pour l'entreprise et les dirigeants la nécessité de bien gérer la structure d'organisation du projet et de s'assurer de l'adhésion des utilisateurs à la technologie développée.

Actuellement, les firmes ont à composer à distance avec des partenaires virtuels. Une telle mutation vers les réseaux de communication basés sur la technologie Internet sous-tend par conséquent un processus de changement organisationnel d'envergure qu'il importe de bien gérer (Franklin, 1997). Selon Franklin (1997 : 3), « Étendre l'Intranet à l'extérieur de l'organisation serait semblable à un projet de re-engineering. » Pareillement, Laudon et Laudon (2000) décrivent l'Extranet comme étant une extension des frontières de l'organisation. En effet, les employés peuvent résister à ce changement, ce qui risque d'entraver et de retarder l'exploitation du réseau de communication mis en place.

Pour résoudre l'ensemble de ces questions, les attentes des employés et des partenaires doivent être prises en considération en premier lieu (Barnes, 2001). Si les utilisateurs ne trouvent aucune utilité dans l'utilisation des réseaux de communication, ils vont l'abandonner. La clef serait de trouver l'interface commune et idéale entre les objectifs organisationnels et personnels. Dans ce sens, McLaughlin (2003) pense qu'il est important d'organiser des rencontres avec tous les intervenants dans l'organisation ayant un recours potentiel à ces réseaux. Il s'agit d'interviews non structurés avec les utilisateurs potentiels. Les questions doivent porter généralement sur la façon par laquelle les différentes divisions de l'organisation interagissent, les moyens de communication avec les partenaires ainsi que les informations sollicitées par ces utilisateurs dans leur fonctionnement. De telles rencontres sont de nature à sensibiliser les utilisateurs potentiels de l'utilité des réseaux de communication basés sur le Web pour l'entreprise et de ses répercussions positives sur la communication aussi bien interne qu'externe.

Comme nous venons de le voir précédemment, Jones (1994) notait que le soutien initial de la part des hauts dirigeants et de l'ensemble des utilisateurs est important pour couronner de succès le développement de n'importe quelle technologie d'information. Sur un autre plan, McLaughlin (2003) pense qu'un tel soutien de la part des utilisateurs potentiels de la TI permettrait aux concepteurs de bien comprendre les politiques de l'entreprise, ce qui représente un facteur critique pour la réussite de l'implantation.

Pour Ward (2003), il serait opportun d'employer les tactiques de marketing afin de stimuler l'accès aux réseaux de communication au sein de l'entreprise de la part de l'ensemble des employés (messages électroniques, diffusion d'articles, promotion, sessions de formation, conférences internes, soutien de la direction, primes, etc.). Fitcher (2003) évoque dans ce cadre le concept de l'« Intranet Marketing » dont l'objectif est d'accélérer l'adoption de la technologie Intranet au sein de l'organisation en donnant aux employés une raison pour utiliser cet outil. Il est indispensable alors de créer un plan de marketing qui soit bien conçu.

Ainsi, il est clair que l'adoption de la technologie Internet soulève un certain nombre de questions relatives à la nécessité de gérer les risques qu'y sont associés. En effet, les questions de

prévention des fraudes, de responsabilisation et de la performance du réseau sont cruciales pour l'entreprise. Plus encore, cette dernière joue sa survie dans le cas où ces risques ne soient pas gérés de la meilleure façon. Ainsi, il serait difficile pour l'organisation de répondre à l'ensemble de ces risques à la fois. Il s'agit d'accorder la priorité aux risques ayant une forte probabilité d'occurrence et à grand impact sur le projet lors de leur réalisation. Pour ce faire, les dirigeants doivent procéder au préalable à une analyse des risques et de leurs impacts. La section qui suit est consacrée à la présentation des différentes approches et méthodes devant être utilisées dans le but d'effectuer une analyse et une évaluation des risques identifiés.

2.4.3 L'analyse et l'évaluation des risques

Le modèle explicité dans la section précédente fournit un cadre de référence quant à l'identification des risques relatifs au développement des technologies d'information au sein de l'entreprise. L'étape suivante consiste à étudier ces risques et à déterminer les menaces et les opportunités qui demandent une réponse (Buttrick, 2002). Il s'agit d'adopter une approche d'analyse et d'évaluation des risques identifiés dans la première étape.

Une fois identifié, il y aura pour chaque risque la détermination de la probabilité d'occurrence ainsi que l'impact attendu. Par la suite, il faut procéder à l'établissement d'un ordre de priorité pour les risques afin d'en formuler une stratégie de gestion efficace (à quel risque faut-il répondre en premier ?). Cela sera déterminé à partir de la tolérance des dirigeants envers les risques identifiés. Pour Feringa et al. (2001), il s'agit de la détermination de la vulnérabilité de l'organisation face aux impacts des risques identifiés. Ces derniers précisent les différents impacts pouvant survenir :

1) Perte d'intégrité : il s'agit de changements inappropriés apportés d'une façon intentionnelle ou accidentelle au contenu informationnel de la technologie d'information développée. Cela serait dangereux pour l'organisation dans la mesure où il peut causer la prise de décisions erronées ou même des fraudes.

2) Perte de disponibilité de la technologie : cela signifie que les utilisateurs potentiels pourraient ne pas exercer les fonctionnalités de la technologie d'information développée.
3) Perte de confidentialité : il s'agit des accès non autorisés au contenu confidentiel de la technologie développée.

Marchewka (2003) et Feringa et al. (2001) proposent deux approches, qualitative et quantitative, quant à l'analyse et l'évaluation des risques.

Premièrement, l'analyse qualitative des risques adopte une vision subjective basée sur l'expérience et le jugement des responsables du projet. Dans ce sens, l'approche qualitative sera d'autant plus efficace si elle est conduite par l'ensemble de l'équipe et non par certains individus, et ce, dans le but d'assurer un échange fructueux des différents points de vue. Feringa et al (2001) identifient certains impacts pouvant être appréciés qualitativement comme la perte de la confiance auprès de la clientèle, la perte de crédibilité, les dommages causés pour les intérêts de la firme, etc. Dans le cadre de l'approche qualitative, plusieurs techniques peuvent être utilisées. Ainsi, le concept de la « valeur espérée » (expected value) représente un outil fiable pour l'analyse du risque. Il consiste en un jeu de probabilités relatives à l'occurrence d'un risque donné. Il permet d'avoir une idée précise sur l'impact du risque – en cas de sa réalisation – en terme monétaire. Les responsables peuvent recourir également aux arbres de décision pour évaluer l'impact des différentes décisions pouvant être prises dans le cadre d'un risque donné. L'arbre de décision fournit un aperçu graphique et visuel sur les différentes décisions et leurs impacts en terme monétaire. L'inconvénient de cette méthode qualitative c'est qu'elle ne chiffre pas les impacts, ce qui serait de nature à rendre difficile d'effectuer une analyse coûts-bénéfices sur les mesures de contrôle à adopter.

Deuxièmement, l'approche quantitative est dédiée à l'évaluation des impacts relatifs aux risques pouvant être mesurés quantitativement tels que les manques à gagner, le coût de réparation, etc. L'approche quantitative inclut des techniques mathématiques et statistiques permettant de modeler la situation de n'importe quel risque rencontré. Les distributions de probabilité sont à la base des modèles conçus. Une fois les probabilités d'occurrence des risques

identifiés ainsi que leurs impacts étudiés, l'entreprise doit répondre à ces risques en optant pour une stratégie visant la réduction et la limitation de ces effets adverses. Dans ce cadre, les auteurs ont avancé plusieurs stratégies que nous présentons dans la prochaine section.

2.4.4 Les stratégies de gestion des risques

Suite à l'analyse et l'évaluation des impacts relatifs aux risques, l'organisation est appelée à concevoir une stratégie en vue de gérer ces risques. Marchewka (2003) précise que l'organisation n'a pas d'intérêt à répondre à tous les risques dans la mesure où ça peut constituer un gaspillage de ressources. Selon Marchewka (2003), la stratégie de gestion d'un risque particulier dépend de certains facteurs à savoir la nature du risque, l'impact du risque sur l'atteinte des objectifs du projet, les contraintes du projet en termes d'envergure, de calendrier, de budget et de qualité, et enfin, les tolérances et les préférences pour le risque de la part des parties prenantes dans le projet.

Dans l'objectif de répondre aux risques identifiés, l'organisation peut adopter l'une des stratégies suivantes avancées par Marchewka (2003) et Feringa et al. (2001) et alimentées par les apports d'autres auteurs. Il s'agit de quatre stratégies possibles à savoir, accepter ou ignorer, éviter, atténuer et transférer. Dans ce qui suit, nous explicitons l'ensemble de ces stratégies :

2.4.4.1 Accepter ou ignorer

Il s'agit de la stratégie la plus passive qu'une entreprise peut adopter dans le cadre de sa gestion du risque. Les responsables espèreront que le risque ne se réalisera pas sans rien entreprendre de leur part. Cependant, il peut s'agir de risques dont la probabilité d'occurrence est tellement faible que les dirigeants n'accepteront pas d'engager des ressources supplémentaires pouvant se révéler injustifiés si le risque ne se réalise pas. Par ailleurs, les réserves stratégiques[13],

[13] Les réserves stratégiques représentent un montant calculé en dehors du budget du projet dont la raison d'être est de faire face aux imprévus.

les réserves d'urgence[14] ainsi que les plans d'urgence[15] peuvent être utiles quant aux risques à faible probabilité de réalisation mais ayant un grand impact sur le projet. Buttrick (2002) ajoute que les risques relativement faibles en termes de probabilité de réalisation et d'impact sur le projet, doivent être surveillés de près sans procéder pour autant à aucune mesure de contrôle.

2.4.4.2 Éviter

La stratégie d'évitement consiste en un certain nombre de mesures entreprises par l'équipe de projet afin d'éviter un risque bien déterminé. Il s'agit de réagir d'une façon proactive pour éliminer toute possibilité de réalisation de ces risques. Ainsi, les responsables du projet vont tout simplement éliminer la cause ou la conséquence du risque.

2.4.4.3 Atténuer

La stratégie d'atténuation consiste à diminuer la probabilité de réalisation des risques. Cette stratégie consiste en la mise en place de certaines mesures de contrôle visant la réduction des effets adverses des risques en cas de leur réalisation, telles que les mesures de sécurité d'accès à l'utilisation de la technologie. Le recours à cette stratégie requiert la présence préalable d'une planification appropriée des différents risques. Feringa et al (2001) pensent qu'il serait important de mener une analyse coûts-bénéfices dans l'objectif d'évaluer l'opportunité des mesures de contrôle à adopter. Une telle analyse touchera à trois volets à savoir : l'impact de l'implantation de la mesure de contrôle, l'impact de la non implantation de la mesure de contrôle et les coûts associés.

Feringa et al (2001) regroupent les mesures de contrôle sous deux catégories majeures. Premièrement, il s'agit des **mesures techniques de contrôle**. Ces mesures tiennent compte de la structure de la technologie à savoir ses ressources logicielles et matérielles. Les mesures techniques de contrôle doivent être entreprises d'une façon conjointe afin de sécuriser les

---

[14] Les réserves d'urgence : il s'agit de fonds mis à la disposition du gestionnaire de projet et figurant dans le budget du projet.

[15] Les plans d'urgence (ou plans de remplacement) : ce sont des plans de dernier recours dans le cas d'un événement indésirable qui se réalise.

données stratégiques. L'adoption de mesures de contrôle techniques permet également de soutenir les paramètres de sécurité de la technologie d'information implantée d'une part et pour prévenir et corriger les problèmes avant qu'ils ne deviennent sérieux d'autre part (ex : l'authentification, l'autorisation, le contrôle d'accès, la non-répudiation, etc.).

Deuxièmement, il est possible d'opter pour des **mesures managériales de contrôle**. Ces mesures de contrôle sont menées dans le but de réduire les pertes potentielles et d'assurer le respect de la mission et des orientations stratégiques de l'organisation. Les mesures managériales de contrôle consistent en l'établissement de politiques visant la protection des informations ainsi que la définition de standards et de plans d'action pour le personnel et l'ensemble des utilisateurs potentiels de la technologie une fois implantée.

Greenstein et Vasarhelyi (2002) avertissent les dirigeants de ne pas resserrer les mesures de contrôle dans le sens où cela risque de créer certaines situations indésirables comme la bornage de la flexibilité de l'entreprise, l'augmentation de l'inefficacité des opérations, l'accroissement des coûts de contrôle et la démotivation des employés. Selon ces auteurs, cela nécessite de concevoir une politique de gestion du risque tenant compte de l'efficacité des technologies de l'entreprise et n'affectant pas par ailleurs sa flexibilité.

D'autres auteurs que nous présenterons dans la sous-section suivante, pensent qu'il est plus avantageux de mandater à une autre partie la gestion des risques dans le but d'éviter l'engagement de ressources importantes et de bénéficier également de l'expérience et de la compétence des experts du domaine des technologies d'information.

2.4.4.4 Transférer

Il y a plusieurs façons de transférer le risque soit premièrement de transférer le risque à une autre partie par le biais de l'assurance (Hoyt et Khang, 1999 et Doherty, 1985) ; deuxièmement, de confier la réalisation de l'ensemble ou d'une partie du projet à un opérateur externe : sous-traitance ou impartition (Laudon et Laudon, 2000 ; Poitevin, 1999 et Leibenstein, 1966) et

troisièmement d'avoir recours au développement par l'utilisateur final (Lebrun, Rivard et Talbot, 1990).

Premièrement, l'assurance des moyens de production constitue un moyen efficace qui permet d'atténuer la vulnérabilité de l'entreprise face aux désastres et aux pertes. Selon Hoyt et Khang (1999), l'assurance désigne toutes formes d'assurance portant sur les actifs ou les moyens de production de la firme. En effet, l'assurance permet d'indemniser l'ensemble des dommages subis par le personnel et ceux causés au reste des moyens de production (matériel, machines, logiciels, etc.) Ainsi, pour Doherty (1985), l'assurance garantit même la survie des organisations par le biais d'un transfert du risque de l'assuré vers l'assureur.

Deuxièmement, l'impartition ou la sous-traitance consiste « à confier la gestion des activités du centre informatique, des réseaux de télécommunications ou de l'élaboration des applications à des fournisseurs externes » (Laudon et Laudon, 2000). Poitevin (1999 : 32) avance qu'« une entreprise est confrontée au choix de produire elle-même ou de se procurer sur les marchés des centaines de biens et services. On conçoit aisément qu'elle aura avantage à se concentrer sur certaines compétences-clés, sur des activités pour lesquelles elle possède un avantage compétitif marqué et sur des domaines pour lesquels ses équipes de direction disposent d'un avantage dans la prise de décision. Pour cette raison, toute entreprise trouvera profitable de confier à des impartiteurs, s'il s'en trouve, la tâche de lui procurer une vaste gamme de biens et services, de composants et de sous-systèmes ». Actuellement, l'impartition des technologies connaît un essor considérable. Évidemment, plusieurs facteurs expliquent le recours accru à l'impartition dans les projets d'informatisation. Premièrement, il s'agit de la veille technologique. En effet, l'évolution de la technologie conduit de plus en plus les entreprises à impartir. En effet, les manières de faire changent constamment dans plusieurs industries ce qui nécessite des compétences particulières pour l'exécution de certaines activités. De telles compétences ne sont pas nécessairement présentes à l'intérieur de l'entreprise qui se veut réaliser un projet d'informatisation. Un tel constat pousse ces entreprises à privilégier l'impartition aux dépens d'une formation continue devant être offerte à ses employés et dirigeants. Opter pour la formation du personnel risque de se révéler coûteux pour l'entreprise (Chevalier, 2001). Deuxièmement, certains auteurs ont avancé les économies d'échelle comme facteur favorisant la sous-traitance ou l'impartition. Selon

Poitevin (1999), un fournisseur travaillant pour plusieurs clients simultanément est censé réaliser plus d'économies d'échelle. Il s'agit d'économies techniques se traduisant par des capacités de production plus importantes qui réduisent substantiellement les coûts. Au fur et à mesure qu'une entreprise produit un bien ou un service, les imperfections dans la production, inévitables au début de la production d'un nouveau produit, sont peu à peu supprimées ou au moins atténuées : le rythme de production s'accroît, le niveau de qualité également. Sur un autre plan, Laudon et Laudon (2000) ajoutent que l'impartition permet à l'organisation de se libérer d'une partie de sa charge de travail et de se consacrer aux activités susceptibles de lui générer un avantage concurrentiel. Troisièmement, la compétition représente l'un des buts les plus recherchés par les entreprises à travers l'impartition de ses projets d'informatisation. En effet, les employés seront enclins à améliorer leurs performances dans la mesure où leur effort de travail sera soumis à la menace de concurrence externe représentée par l'effort du fournisseur potentiel. Selon Helper (1991), la compétition serait génératrice d'innovation. Dans ce sens, la concurrence permettrait à l'entreprise de réduire et de limiter les risques d'inefficacités durant l'exécution de ses projets d'informatisation.

Troisièmement, selon Davis et Olson (1985), le développement des TI par l'utilisateur final ou l'informatique de l'utilisateur se définie comme étant « l'automatisation du poste de travail par l'utilisateur lui-même, grâce à un ensemble d'outils informatiques et de moyens de support ». L'informatique de l'utilisateur a apporté des solutions aux problèmes clefs de l'informatique.

Dans la plupart des organisations, l'implantation de l'informatique utilisateur a pu apporter des changements considérables. Ces changements portaient sur les outils de communication, l'utilisation de l'information, la préparation des rapports, la prise de décisions, les rôles des intervenants, etc. (Lebrun, Rivard et Talbot, 1990). Au niveau de l'organisation, le recours a l'informatique utilisateur serait de nature à améliorer la productivité de ses employés (Alavi, 1985), de perfectionner la prise de décision (Kasper, 1985, Moreau, 2000) et d'optimiser sa rentabilité (Keen, 1983).

L'implication de l'utilisateur constitue un ingrédient indispensable afin de couronner le succès du développement des technologies au sein des organisations (Barki et Hartwick, 1990).

Toutefois et en dépit des gains qu'offre l'informatique de l'utilisateur, cela ne peut cacher les insuffisances de cette technique. Davis (1982) rappelle que les utilisateurs ne disposent pas de la même formation que les professionnels en matière de technologies d'information. Par conséquent, les applications développées par les utilisateurs peuvent contenir de sérieuses imperfections. Les décisions bâties sur la base de ces applications peuvent être mal fondées, et de telles mauvaises décisions menacent l'avenir de l'organisation.

Par ailleurs, le processus de gestion du risque peut subir certains changements et révisions en fonction de la nature changeante des risques et des aléas imprévisibles durant l'avancement du projet. Par conséquent, il serait préférable d'avoir un œil sur l'exécution du processus en ayant recours à certaines techniques et outils que nous présentons dans la section qui suit.

2.4.5 La surveillance et la réponse aux risques

Une fois le plan de réponse établi, les différents risques doivent demeurer sous une surveillance continue. En effet, d'autres menaces et opportunités peuvent apparaître en cours de route, ce qui interpelle la vigilance des dirigeants. Une fois le risque réalisé, le gestionnaire de projet sera tenu d'entreprendre les mesures nécessaires pour riposter selon la stratégie qu'il a adoptée au début (Marchewka, 2003). Greenstein et Vasarhelyi (2002) pensent que l'avancement de l'implantation de la technologie doit être surveillé durant toutes les phases de développement afin de pouvoir suivre les déviations et les corriger. Les corrections et les rectifications doivent être apportées à l'ensemble du processus de gestion du risque.

La surveillance et le contrôle consistent en la mise en place de certains indicateurs pour renseigner de la réalisation des risques. Dans ce cadre, Marchewka (2003) recommande aux organisations le recours aux techniques suivantes :

1) **L'audit des risques** : interroger le gestionnaire et l'équipe de projet de la part d'un expert ou d'un connaisseur du domaine sur les risques identifiés et les plans de réponses établis. L'audit doit être mené par une partie externe à l'équipe de projet afin de garantir la diversité des idées et le jugement d'experts.

2) **Les révisions** : les révisions suivent le même principe que les audits des risques, sauf qu'elles sont menées par une personne faisant partie de l'équipe de projet.
3) **Les rapports de situation** : il s'agit d'un outil de communication dont l'objectif est de vérifier la rencontre des jalons établis au départ.

Feringa et al (2001) rappellent que la technologie d'information, une fois implantée et mise en marche, sera amenée à subir des modifications et des mises à jour, dans la mesure où certaines composantes seront rajoutées et d'autres plutôt supprimées. Pareillement, des changements dans la structure des ressources humaines compétentes peuvent avoir lieu. Par conséquent, Greenstein et Vasarhelyi (2002) soulignent le fait que le processus de gestion du risque doit être continuel, itératif et évolutif. Dans ce cadre, Feringa et al. (2001) identifient certains facteurs comme le soutien de la direction, la compétence et l'expertise de l'équipe de projet, qui seront d'autant plus indispensables quant à la réussite de la politique de gestion du risque.

En conclusion, nous avons pu voir à travers ce chapitre les différentes notions relatives à la théorie de gestion du risque. D'abord, nous avons examiné les quatre catégories des risques pouvant survenir durant les projets d'informatisation : financier, technique, de coût et d'échéancier. Une telle catégorisation est importante dans la mesure où elle permet aux décideurs de bien identifier les risques et de bien choisir le moyen approprié en vue de le mitiger. Par la suite, nous avons observé la dynamique des risques par rapport aux mesures de contrôle adoptées. Qui plus est, nous avons mis l'accent également sur les facteurs clefs de succès de toute politique de gestion du risque et qui consistent dans le soutien de la direction, les critères de choix de la technologie et la gestion de la structure d'organisation du projet. Enfin, nous avons présenté un processus de gestion du risque ayant adapté les apports de plusieurs auteurs dont principalement Marckewka (2003). En effet, cette approche consiste en un processus destiné à assurer le bon déroulement du projet par la réduction de la probabilité de réalisation des risques identifiés. Le processus que nous avons adapté regroupe un ensemble d'activités interdépendantes visant à limiter au maximum les retombées négatives que peuvent avoir les risques en cas de leur réalisation. Dans le chapitre qui suite, nous exposons notre méthodologie de recherche et nous présentons nos descriptions de cas.

CHAPITRE III : LA MÉTHODOLOGIE DE RECHERCHE

Nous rappelons tout d'abord notre question de recherche qui consiste à identifier les risques relatifs aux projets d'informatisation ainsi que leur pratiques de gestion. Nous proposons également comme objectifs spécifiques de recherche d'étudier les risques et les pratiques de gestion du risque inhérents aux réseaux de communication basés sur la technologie Internet. Dans les sections suivantes, nous présentons la méthodologie de recherche que nous proposons d'effectuer. Dans un premier temps, nous spécifions la nature de notre travail ainsi que la structure de preuve privilégiée selon les recommandations des auteurs reconnus dans le domaine de la recherche méthodologique. Par la suite, nous présentons la méthode de collecte de données. Dans la troisième section, nous traitons la question de l'échantillonnage. Enfin, nous parlons du traitement des résultats.

3.1 La nature de la question de recherche et la structure de preuve choisie

En ayant recours à l'ouvrage de Gauthier (2002) sur la recherche sociale, nous avons pu constater la nature de la question de recherche que nous proposons. Il s'agit en fait d'une recherche **descriptive-exploratoire**. En effet, notre recherche est descriptive à la base dans la mesure où elle se consacre à présenter et à décrire les risques et les pratiques de gestion du risque relatifs aux technologies d'information. Ces risques représentent des situations indésirables que peuvent rencontrer certaines entreprises dans leur activité. Ainsi, nous avons tenté dans la partie théorique de décrire ces situations de risques et en particulier ceux se rapportant à la technologie Internet.

Sur un autre plan, nous décrivons également les pratiques de gestion du risque avancées par certains auteurs. Selon Gauthier (2002), cela s'inscrit dans le cadre de la réaction des organisations face aux évènements imprévisibles. Dans notre cas, ces évènements sont les risques et les pratiques de gestion de ces risques et qui représentent la réaction des organisations à ces derniers. Plus encore, nous avons présenté un processus dédié à la gestion du risque avancé par Marchewka (2003) et que nous avons appuyé par les apports d'autres auteurs dont principalement Feringa et al. (2001) et Greenstein et Vasarhelyi (2002).

Par ailleurs, notre recherche possède aussi un volet exploratoire étant donné que nous cherchons à alimenter et à enrichir notre contenu théorique au niveau des risques et des pratiques de gestion des risques relatifs à l'Internet. Selon Gauthier (2002), la question de recherche exploratoire porte sur un thème peu étudié. Ainsi, cela serait de nature à entraîner certaines modifications et révisions au niveau du cadre conceptuel et de le reformuler en fonction des conclusions tirées à partir des démarches empiriques. Gauthier (2002) qualifie ce type de recherche de constructiviste dans la mesure où elle tente de comprendre davantage un phénomène à savoir les risques et les pratiques de gestion du risque. Dans ce contexte, nous cherchons à enrichir et à alimenter davantage les apports théoriques des auteurs dans le but de cerner les approches suivies par les professionnels dans le cadre de la gestion du risque des technologies d'information.

Par contre, Gauthier (2002) soutient qu'une recherche descriptive doit être basée sur une théorie et exhaustive. Dans ce cadre, il pense que la meilleure façon de procéder dans la vérification de cette théorie, serait une structure de preuve basée sur la **description de cas multiples**. Gauthier (2002) continue en avançant que la structure de preuve descriptive permettrait de traiter plusieurs cas afin d'approfondir et d'appuyer les résultats. Toutefois, il précise que l'inconvénient majeur de cette stratégie est le fait qu'elle requiert plus d'efforts distribués sur plusieurs sujets. Par ailleurs, une telle structure de preuve descriptive demande de la mise en application de certaines méthodes de collecte de données telles que les observations directes et les entrevues semi-dirigées. Cependant, le recours aux observations n'est pas possible dans notre cas parce que cela demande notre présence durant le déroulement de toutes les phases de développement du projet. De plus, les observations limiteront notre étude à un seul projet par entreprise. Par conséquent, nous avons opté pour les **entrevues semi-dirigées**. En effet, à travers cette méthode de collecte de données, nous aurons la possibilité d'avoir les témoignages de plusieurs dirigeants ayant mené une multitude de projets d'informatisation dans leurs carrières et de comprendre les approches de gestion du risque qu'ils valorisent. Ainsi, nous serons en mesure d'approfondir notre étude des risques et des modes visant leur gestion. Dans ce qui suit, nous présentons les justifications du recours à cette méthode de collecte des données.

3.2 La méthode de collecte des données : les entrevues semi-dirigées

Dans le cadre de notre travail de recherche, nous aurons recours aux entrevues semi-dirigées pour la collecte des données. Certains auteurs que nous verrons dans ce qui suit ont appuyé ce choix pour les recherches descriptives et exploratoires. De plus, la plupart des auteurs que nous avons présentés dans la partie théorique de ce travail, ont eu recours à cette méthode dans leurs études. En effet, des auteurs comme Ward (2003), McLaughlin (2003) et Marchewka (2003) ont eu recours à leurs expériences personnelles pour présenter les risques et leurs méthodes de gestion. Par ailleurs, ces derniers ont appuyé leur profil personnel par les entrevues semi-dirigées pour approfondir les connaissances sur le sujet étudié. Les objectifs poursuivis à travers l'utilisation de cette méthode de collecte de données tournent autour de la découverte, la compréhension et l'apprentissage (Gauthier, 2002). Ainsi, nous aurons la chance d'élargir le champ des connaissances relatives à la gestion du risque des technologies d'information.

Gauthier (2002) pense qu'il importe d'effectuer des entrevues semi-dirigées quand il s'agit de recherche exploratoire, comme dans notre cas. Il précise qu'une recherche de type exploratoire a pour but de construire une théorie ou un ensemble de concepts concernant un phénomène donné. Selon la définition de Gauthier (2002), l'entrevue « consiste en une interaction verbale entre des personnes qui s'engagent volontairement dans pareille relation afin de partager un savoir d'expertise et ce, pour mieux comprendre un phénomène d'intérêt pour les personnes impliquées » (Gauthier, 2002 : 265).

En effet, nous avons besoin dans le cadre de notre travail de recherche d'une certaine interactivité et échange avec les répondants dans l'objectif de bien comprendre les approches utilisées par ces professionnels. Egalement, ces derniers cherchent aussi à discuter leurs idées et à les confronter aux arguments théoriques avancés par plusieurs auteurs. Dans ce cadre, nous présenterons aux répondants, tout au long du déroulement de l'entrevue, les contreparties théoriques de leurs approches, et ce, en vue de générer plus d'interactivité et d'assurer un échange constructif et fructueux durant la rencontre.

Par contre, Gorden (1980) pense que le rôle du répondant sera « celui d'un participant actif qui évolue dans ses réflexions grâce à l'aide du chercheur-expert » (Gauthier, 2002 : 271). Dans ce cadre, nous avons développé un guide d'entrevue comportant un ensemble de 16 questions ouvertes (voir l'annexe A). Bien évidemment, les questions concernent tout le contenu théorique avancé. En effet, ce guide a été élaboré à partir de nos questions de recherche et de notre cadre conceptuel. Ainsi, notre guide repose sur la structure théorique de notre recherche. Le but étant de confronter les apports de certains auteurs à ce qui se passe au sein de certaines firmes québécoises. Cela serait de nature à enrichir la théorie de gestion du risque avancée, et ce, en recensant les risques les plus rencontrés au Québec ainsi que les pratiques de gestion du risque les plus utilisées dans ce cadre.

Les questions 1 et 2 sont consacrées à constater l'apport des technologies d'information et en particulier l'Internet, au niveau du fonctionnement de l'entreprise étudiée. La question 3 aura comme finalité de décrire le niveau de soutien accordé par la direction aux réseaux de communication basés sur Internet. Les questions 4, 5 et 6 traiteront des critères de choix auxquels l'entreprise s'est fiée durant l'adoption de la technologie Internet. En fait, les critères avancés dans la théorie sont la rentabilité et l'ajustement de la technologie à la stratégie de l'entreprise. Ainsi, il serait possible à travers les réponses d'alimenter le contenu théorique en incluant d'autres critères de sélection pertinents. À travers la question 7, nous essayerons de voir et d'évaluer la façon par laquelle l'entreprise gère la nouvelle structure organisationnelle induite par l'adoption d'Internet dans la mesure où cela change les frontières de l'organisation et de l'environnement du travail. Par la suite, la question 8 fera le tour des risques ayant été rencontrés par les répondants dans le but de préciser les risques spécifiques pour chaque répondant et de les expliciter. Cela nous amène à poser les questions 9 et 10 relatives à la présence ou non d'une politique ou d'un processus standard de gestion du risque au sein de l'entreprise. Ainsi, nous serons en mesure de comparer ce processus à celui avancé dans la théorie et d'en constater les différences.

Les questions 11 à 16 tenteront de vérifier l'application des activités ou des éléments qui composent les différentes phases du processus de Marchewka (2003) à savoir la planification, l'identification des risques, l'analyse et l'évaluation des impacts, l'emploi de la stratégie de

gestion du risque et la surveillance du processus. Dans ce cadre, nous avons eu recours à l'illustration graphique que nous avons adapté de Marchewka (2003)[16] et qui présente les différentes phases ainsi que les éléments y afférents. En effet, une telle référence graphique est susceptible de bien orienter nos recherches et nos observations empiriques.

Une fois les méthodes de collecte de données définies, il importe de penser aux entreprises qui seront décrites dans le cadre de notre recherche. En effet, il s'agit de choisir ces entreprises sur une base bien déterminée afin d'assurer une certaine représentativité dans l'étude. Cela nous amène donc à nous interroger sur la méthode d'échantillonnage que nous traitons dans la section suivante.

3.3 L'échantillonnage

Les entreprises qui constitueront notre champ d'étude appartiennent à des secteurs spécifiques de services. Nous avons choisi d'établir la description de **trois organisations**. La première étant l'Université du Québec à Trois-Rivières qui opère dans l'enseignement et la recherche. La deuxième organisation décrite est Communication Inc. qui offre des services de marketing et de communication. Enfin, nous décrirons le cas de Telus Solutions d'affaires qui soutient sa clientèle au niveau du positionnement stratégique en leur offrant les outils technologiques et les conseils stratégiques nécessaires.

Il s'agit d'un échantillon typique non probabiliste basé sur le choix de certains individus de la population totale et dont les particularités pourraient être généralisées. Selon Gauthier (2002), « si la recherche se veut **exploratoire**, si ce qui intéresse le chercheur, ce ne sont pas les variations mêmes à l'intérieur de la population, mais plutôt quelques particularités de celle-ci, pour quoi alors chercher une représentativité qui n'aura qu'un intérêt limité ? » (Gauthier, 2002 : 199). Ce dernier ajoute également que l'échantillon typique représente une technique non probabiliste par choix plutôt que par défaut. En effet, étant donné la nature exploratoire de notre recherche empirique, il importe de choisir des cas d'entreprises ayant déjà eu recours à la technologie Internet et ne présentant « aucun trait particulier, exceptionnel susceptible d'affecter

[16] Voir la figure 2.

fortement le phénomène étudié » (Gauthier, 2002 : 200), et ce, afin d'étudier leur approche de gestion du risque et de pouvoir confirmer ou infirmer une théorie.

Dans ce cadre, notre échantillon a été établi à partir de nos contacts personnels. Le répondant relatif à notre premier cas de l'UQTR, le directeur chargé du développement des systèmes d'information au sein du service de soutien pédagogique et technologique, a été contacté par courriel et par téléphone. Le choix s'est porté en premier sur l'UQTR étant donné qu'il s'agit de l'établissement qui nous est le plus proche et qui représente pour autant une organisation qui a constamment recours aux nouvelles créations technologiques. Tandis qu'aux données relatives au deuxième cas, elles ont été recueillies grâce aux démarches qui ont été déployées par une ex-employée chez Communication Inc., qui nous a organisé une rencontre avec l'ex-directrice du département des TI de la compagnie. Quant à la troisième firme étudiée, Telus solutions d'affaires, c'est grâce aux efforts d'une professeure à l'UQTR dont le champ de compétences sont les systèmes d'information, que le directeur principal chez Telus Solutions d'affaires, a été contacté et nous a fait part de l'approche de gestion du risque appliquée par sa compagnie. Nous notons dans ce cadre que nous avons les noms réels de l'UQTR et de Telus solutions d'affaires. Par contre, le nom de la deuxième entreprise a été changé pour Communication Inc., et ce, pour des raisons de confidentialité.

Dans ce sens, nos répondants contribueront à enrichir le contenu théorique relatif aux pratiques de gestion du risque et à nous renseigner également sur les particularités de ces pratiques dans leur secteur d'activité respectif. En effet, un tel choix est imposé par la nature descriptive-exploratoire de notre travail de recherche qui nécessite de faire le tour des différentes approches et méthodes adoptées par les professionnels. Par conséquent, il nous revient de bien approfondir ces études de cas dans le but de collecter le plus d'informations sur les risques et leurs pratiques de gestion dans les différents secteurs d'activité au Québec. Cela nous amène à nous interroger sur la façon par laquelle les résultats seront traités.

3.4 Le traitement des résultats

Dans notre recherche, il s'agit de vérifier l'existence de certains éléments bien déterminés ayant trait aux risques et à la politique de leur gestion au sein des entreprises étudiées. La figure 2 relative à notre cadre conceptuel réunit l'ensemble de ces éléments puisés à partir de la théorie. Ainsi, les résultats seront traités qualitativement. En effet, les données recueillies seront organisées selon l'enchaînement logique de notre cadre théorique, et ce, dans la mesure où nous tenterons dans un premier temps d'identifier les éléments sur lesquels repose la politique de gestion du risque du répondant. Dans un deuxième temps, ces éléments seront confrontés aux arguments présentés par les auteurs pour être discutés. Par ailleurs, à partir des réponses collectées, nous sommes en mesure d'identifier les principales TI basées sur Internet auxquelles les entreprises ont recours pour en juger leur volonté à les utiliser dans leurs activités. De plus, nous observerons la présence des facteurs clefs de succès notamment le soutien de la direction, les critères de choix de la technologie et la gestion de la structure d'organisation du projet. Sur un autre plan d'analyse, nous déterminerons les principaux risques spécifiques au domaine d'activité de nos répondants. Également, nous discuterons les méthodes de gestion du risque telles que déployées par les répondants et nous commenterons l'approche qu'ils valorisent dans ce cadre.

Dans ce chapitre, nous avons exposé la méthodologie de recherche que nous utiliserons dans le cadre de la recherche empirique. Premièrement, nous avons démontré la nature descriptive-exploratoire de notre question de recherche et nous avons déduit la structure de preuve privilégiée : les descriptions de cas, et ce, telle que préconisée par Gauthier (2002). Deuxièmement, nous avons prouvé le choix de la méthode de collecte de données, à savoir les entrevues semi dirigées. Enfin, nous avons présenté notre plan d'échantillonnage ainsi que la méthode de traitement des résultats. Toutefois et dans le but d'appuyer notre analyse empirique, nous avons élaboré une grille d'évaluation des réponses basée sur une comparaison entre les arguments théoriques et ceux des répondants. Dans le cadre de cette grille, nous avons noté les auteurs respectifs ayant traité les éléments[17]. Le quatrième chapitre qui suit présente les trois cas que nous avons décrits. Sur un autre plan, nous commentons l'ensemble des conclusions que nous avons pu tirer au sujet des risques et de la politique de gestion du risque de nos répondants.

---

[17] Voir l'annexe B.

CHAPITRE IV : LES DESCRIPTIONS DE CAS

Nous essayerons dans le cadre de ce chapitre de voir de quelle façon certaines firmes québécoises appliquent leurs approches de gestion du risque, et ce, après avoir identifié et catégorisé les risques qu'elles rencontrent. Dans ce cadre, nous présenterons une description de nos répondants et de leurs secteurs d'activités respectifs, les principales TI auxquelles ils ont recours et la méthode de gestion du risque déployée. Enfin, nous ferons part de nos commentaires et nous illustrerons à l'aide de graphiques chacune des approches telle qu'appliquées par nos répondants.

4.1 Cas 1 : L'Université du Québec à Trois-Rivières

4.1.1 La description de l'entreprise[18]

Membre du réseau de l'Université du Québec, l'Université du Québec à Trois-Rivières, qui est notre premier cas, représente le secteur de l'enseignement. Fondée en 1969, l'UQTR est l'unique institution universitaire dans la région de la Mauricie[19]. En effet, Trois-Rivières est une des plus grandes villes au Québec avec 125,000 habitants. Elle est reconnue notamment par son caractère industriel notamment l'industrie des pâtes et papiers.

L'UQTR accueille plus de 10,000 étudiants répartis entre 150 programmes de premier, deuxième et troisième cycles. Les formations offertes se rapportent à plusieurs domaines dont le génie (génie mécanique, génie électrique et génie industriel), les sciences de la gestion, la comptabilité, la chiropratique, l'éducation physique, la biologie médicale, etc. également, l'UQTR reçoit des étudiants étrangers en provenance de 37 pays, en particulier les pays francophones.

---

[18] Les chiffres et les données ont été puisés à partir du site Web de l'UQTR (www.uqtr.ca) ainsi que d'autres brochures et livrets de promotion.

[19] L'effectif de l'UQTR s'élève à 1200 employés

Les départements sont décentralisés au niveau de leur fonctionnement. Dans ce sens, chaque département dispose d'un budget bien déterminé afin de mener ses projets, en particulier les projets de recherche[20]. Sur un autre plan, l'UQTR accueille et soutient plusieurs instituts de recherche comme l'Institut de la recherche sur les PME, le Centre de recherche sur l'hydrogène, etc.

Sur un autre plan, l'UQTR est en partenariat avec plusieurs organismes que ce soit à l'échelle provinciale, nationale et internationale[21]. Dans ce cadre, les partenariats sont très étroits avec les entreprises de la région de la Mauricie qui bénéficient des compétences formées dans les locaux de l'UQTR. En effet, cette dernière adapte ses programmes aux évolutions du marché de l'emploi afin d'offrir des possibilités d'embauche pour ses étudiants par la suite. Dans les paragraphes qui suivent et en s'appuyant sur les entrevues réalisées avec le directeur chargé du développement des systèmes d'information au service de soutien pédagogique et technologique et le directeur du service de soutien pédagogique et technologique de l'UQTR[22], nous ferons le tour des principales TI auxquelles fait recours l'UQTR et leurs apports pour cette dernière. Nous présenterons aussi l'approche de gestion du risque telle que mise en application par l'institution et nos commentaires formulés sur la base de la grille d'évaluation présentée à l'annexe B.

4.1.2 Les principales TI et leur place dans l'organisation

L'UQTR dispose tout d'abord d'un site Internet conçu dans le but de promouvoir son image de marque auprès des étudiants, des partenaires, des entreprises et même des employés. Le site Web de l'Université offre plusieurs services dont principalement les inscriptions en ligne pour les étudiants. En effet, en 1999 l'UQTR était la première université québécoise à avoir offert ce type de service à ses étudiants. Plus encore, il est possible de remplir des demandes d'admission via le site Web de l'UQTR, ce qui revient plus rapide et moins coûteux surtout pour les candidats demeurant à l'étranger. Ce site offre également des renseignements sur les programmes assurés par l'Université, la description des cours, les avis et les communiqués de l'administration, les

[20] Il y a près de 295 projets de recherche en cours répartis sur 24 unités de recherche.
[21] Plus de 200 entreprises et organismes sont en partenariat avec l'UQTR.
[22] Cette entrevue a été effectuée en novembre 2002 par M. Pavel Zoubarev, étudiant en maîtrise de gestion de projet à l'UQTR.

résidences sur Campus, les partenaires, la ville de Trois-Rivières, etc. Les entreprises sont en mesure de communiquer plus aisément avec les départements de l'UQTR et de connaître les pistes possibles de partenariat. De plus, le corps professoral, les étudiants ainsi que le personnel de l'UQTR disposent de courriers électroniques à l'adresse de l'Université (nom de la personne@uqtr.ca). Les départements de l'UQTR bénéficient de sites Web dérivés. Certains professeurs ont même la possibilité de concevoir des sites Web personnels. Ainsi, ces derniers sont en mesure de stocker leurs fichiers et documents et de les offrir aux étudiants. Ils peuvent même afficher les résultats d'évaluation sur ces sites Web.

Quant aux employés de l'UQTR, ils ont accès à un Intranet pour gérer leurs tâches et pour améliorer leurs modes de fonctionnement et de communication. Actuellement, ces derniers gèrent de plus en plus leurs tâches via Intranet. Les utilisations de l'Intranet se rapportent à la circulation et au partage de l'information, aux courriers électroniques et la gestion de la documentation. Les apports de l'Intranet pour l'UQTR se situent à plusieurs niveaux : la finance et la comptabilité, les ressources humaines, les évaluations des étudiants, etc.Tous les utilisateurs au sein de l'UQTR (professeurs, employés et étudiants) ont un accès libre et illimité au réseau Internet, et ce, via 350 postes connectés. Également, nous notons la présence de 30 salles équipées d'outils multimédia, une salle de vidéoconférence et de deux laboratoires multimédia d'enseignement des langues. Cependant, la place primordiale qu'occupent les TI dans le fonctionnement de l'UQTR implique normalement une présence de certains risques qu'il importe de gérer. Dans la sous-section suivante, nous découvrions les risques auxquels fait face le département des TI de l'UQTR ainsi que leurs modes de gestion.

4.1.3 Les risques relatifs aux réseaux basés sur Internet et leurs modes de gestion

Il existe un département de soutien technologique et pédagogique comprenant au total 55 employés ayant comme mission de développer des applications technologiques au sein de l'université. Le département est soutenu par la direction de l'université qui est à l'origine de la majorité des mandats qui lui sont adressés. Les responsables du département sont conscients des retombées positives que peuvent avoir les TI en général sur leurs modes de fonctionnement et sur leur rendement. Ils manifestent une détermination à acquérir les nouvelles créations

technologiques et à bien maîtriser les avancées qui ne cessent de se réaliser dans ce domaine extrêmement dynamique. Par ailleurs, le département des TI de l'UQTR fait appel souvent à des ressources de l'extérieur pour élargir ses connaissances existantes à travers des séances de formation assurées par ces derniers.

Comme nous l'avons vu dans le deuxième chapitre, le soutien de la direction représente le premier facteur clef de succès pour tout effort de développement technologique (Jones, 1994), en particulier en ce qui a trait aux réseaux de communication basés sur Internet. Dans ce cadre, les ressources interviewées affirment que le soutien de la direction de l'Université est très présent. Ils continuent en signalant que la direction avait fait preuve d'un esprit de compréhension et avait fourni tous les moyens nécessaires pour l'avancement du projet. Le département des TI travaille en constante et étroite collaboration avec les différents responsables ayant mandaté la mise en place du réseau. Ces derniers font quasiment partie de l'équipe projet, du fait qu'ils sont les utilisateurs potentiels de cette technologie.

Quant au choix de la technologie, le département avait à choisir entre l'Internet et la technologie client-serveur. Toutefois, cette dernière était relativement dépassée et obsolète. Les fonctionnalités qu'offrait la technologie client-serveur étaient moins pratiques que celles offertes par Internet. Par ailleurs, le principal critère ayant conclu le choix de la technologie Internet était l'étude de rentabilité. Cependant, cette étude n'était pas assez développée du fait des avantages inégaux et indéniables que représentait cette technologie. L'importance des investissements requis avait été négligée par rapport aux avantages escomptés.

Sur un autre plan, l'évaluation de ces réseaux a été établie également sur la base de leurs apports au niveau stratégiques pour l'UQTR. Le recours à la technologie Internet avait comme finalité de satisfaire davantage les étudiants qui représentent la principale clientèle de l'Université. Toutefois, le déploiement de ces réseaux était associé avec d'autres politiques ayant comme objectif d'accroître le nombre des étudiants à l'UQTR. Le directeur du service de soutien pédagogique et technologique disait que dans tous les projets qui sont réalisés par le département des TI, l'accent est constamment mis sur la mission de l'Université à savoir l'enseignement et la

recherche. Avant d'approuver le projet de développement technologique, l'équipe examine ses contributions par rapport à la mission et aux objectifs premiers de l'institution.

Plus encore, le département fait souvent recours aux alliances stratégiques dans le domaine du développement technologique dans le but de soutenir les orientations stratégiques de l'UQTR. Dans ce cadre, cette dernière a déjà eu affaire avec le gouvernement du Québec, l'Agence universitaire de la francophonie ainsi que d'autres entreprises québécoises. Également, elle développe même des réseaux en commun avec d'autres universités, et ce, en raison de la forte concentration du savoir-faire et de la capacité d'innovation au niveau des universités.

En ce qui concerne la gestion du changement organisationnel, il est à noter que les équipes de projet oeuvrant sous la tutelle du département des TI de l'UQTR sont multidisciplinaires et proviennent de domaines différents. En effet, ces équipes comportent des ressources ayant des profils en programmation, infographie, applications audiovisuelles, pédagogie, etc. Pareillement, les professeurs, les employés et même certains étudiants interviennent dans tous les projets de développement des réseaux de communication de l'UQTR. Ainsi, le département collabore avec les professeurs pour comprendre leurs problèmes et opter par conséquent pour la solution la plus appropriée comme par exemple dans le cas de la numérisation des notes de cours. La présence de plusieurs intervenants est susceptible de créer certains conflits tels que nous avons présentés dans la section relative à la gestion du changement organisationnel au premier chapitre (Buttrick, 2002 et Marchewka, 2003).

Dans ce cadre, nos répondants affirment que les rencontres entre les membres de l'équipe projet sont fréquentes et régulières dans le but d'assurer de bonnes conditions de travail et de prévenir de tels conflits avec la concertation et l'échange. Plus encore, le directeur chargé du développement des SI au sein de l'UQTR, signale aussi que c'est le chef de projet qui se réserve le droit de donner des directives à l'équipe. Dans ce sens, celles qui émanent de certains directeurs fonctionnels ou partenaires ne sont pas prises en considération par l'équipe sauf à titre de suggestion ou de remarque à discuter.

Plusieurs risques ont été rencontrés lors du développement des réseaux basés sur Internet. Les interviewés disent que le département ne se fie pas à une politique bien déterminée dans la gestion du risque inhérent à ces réseaux. Par contre, les spécialistes dans l'équipe déterminent l'ensemble des éléments qui composent la problématique posée afin de prédire les imprévus en d'autres termes, ils spécifient la technologie d'un point de vue du savoir, du contenu et du matériel demandés. Le client du livrable est tenu au courant de ce qui se dégage comme conclusions et peut même être partie intégrante dans l'identification de ces risques. Pour ce faire, l'équipe de projet fait appel à plusieurs spécialités. S'il y a certains risques importants, en particulier des risques techniques, l'équipe procède au transfert de ces risques à une autre partie plus experte. De plus, les rencontres au sein de l'équipe représentent un moyen privilégié dans la politique de gestion du risque du département des TI de l'UQTR.

De plus, l'équipe de projet développe un plan détaillé des tâches à faire comprenant les activités, les coûts, les échéanciers ainsi que les ressources requises. Par la suite, les rencontres se tiennent à chaque semaine du projet. Il y a même des rapports de situation qui sont élaborés avec des suivis pour les sous-traitants. Les entrevues réalisées avaient permis de recenser certains risques rencontrés par le département des TI de l'UQTR durant le développement des réseaux Internet et qui consiste dans la veille technologique, la définition du contenu de la technologie, la gestion des partenariats, la correspondance de la technologie à la capacité de financement du client, le respect des droits de propriété intellectuelle et l'adhésion des utilisateurs. Ces risques sont détaillés davantage dans ce qui suit.

4.1.3.1 La veille technologique

Il s'agit d'abord de s'assurer que l'équipe maîtrise l'ensemble des applications à développer. Dans ce cadre, les dirigeants pensent qu'ils doivent être en mesure de bien gérer et de présenter au mieux ce qu'ils développent. Souvent, l'équipe de projet procède à la spécification de la technologie. En effet, il y a lieu d'identifier les livrables intermédiaires et de s'organiser en fonction de ces derniers. De plus, l'équipe fait appel aux utilisateurs de cette technologie dans le but de préciser les fonctionnalités requises du fait qu'elle est consciente de la croissance

constante des besoins et de la nécessité de s'adapter à cette croissance en fournissant les réponses appropriées.

Parfois, les connaissances de certains employés du département peuvent être dépassées par rapport aux innovations réalisées dans le domaine des réseaux Internet. Cela nécessite pour les responsables du département des TI de l'UQTR d'effectuer des séances de formation pour ces derniers. Dans ce cadre, l'association avec d'autres universités et partenaires au Québec a permis à l'UQTR de perfectionner et d'améliorer le savoir-faire de son personnel.

Par ailleurs, le projet peut demander plus de temps à être réalisé en raison des révisions qui se font au niveau de sa conception. Cela revient au fait que certaines innovations émergent en cours de route et qu'il serait opportun de les intégrer dans l'exécution du livrable. Néanmoins, la prise en considération de ces innovations peut causer des retards dans la réalisation du livrable.

4.1.3.2 La définition du contenu de la technologie

Une des difficultés les plus communes souvent rencontrées quand il s'agit de développer le réseau Internet de l'UQTR est l'obtention du contenu de la technologie de la part des professeurs et de l'ensemble des utilisateurs potentiels. De plus, le contenu peut être difficile à traiter. Cela pose la question de la faisabilité technique du projet. En effet, ce risque est plus prononcé dans le domaine de la formation universitaire car les informations affichées ne sont pas censées contenir des erreurs. Ainsi, la réussite du projet est tributaire du professionnalisme et de la collaboration de ces derniers. Cela risque de causer des pertes de temps surtout si l'on sait que certains utilisateurs révisent constamment leurs contenus durant le développement. Dans ce cadre, il y a beaucoup de rencontres qui se tiennent dans le but de finaliser et d'améliorer le contenu.

Parfois, ce sont les professeurs qui développent eux-mêmes leurs sites Web personnels. Pour ce faire, le département des TI de l'UQTR organise des ateliers de formation qui consistent à offrir aux professeurs les moyens et les connaissances requises pour le développement de leur propre site Web. Néanmoins, le soutien demeure constant suite à la mise en place du site.

Une autre façon de procéder quand il y a lieu de tel risque, c'est de garder la même structure de la technologie quand il y a des modifications mineures au niveau du contenu. Dans ce sens, l'équipe de projet valide tous les avancements qu'elle fait auprès de son client. En d'autres termes, l'approbation par le client du livrable est nécessaire avant toute nouvelle étape, et ce, afin d'éviter les corrections majeures. Des cautions doivent être versées de la part du client pour prévenir ce genre de risques surtout ceux qui engendrent l'annulation du contrat.

4.1.3.3 La correspondance de la solution adoptée à la capacité de financement du client

Il importe de concevoir une solution qui correspond aux moyens de financement du client. C'est dans ce cadre que s'inscrit la spécification de la technologie et l'élaboration d'un devis détaillé des coûts prévisionnels. Pour ce faire, l'équipe de projet établit un plan d'action comportant l'ensemble des tâches à réaliser. Parfois, c'est l'organisme subventionnel qui impose des normes particulières. Les spécialistes de l'équipe évaluent les besoins du client et élaborent un éventail des solutions possibles. Par la suite, il revient au client du projet de faire le choix de la solution. Nous notons que les gabarits réunissent toutes les étapes concourant à la production de la solution, ce qui fournit un calendrier pour les échéanciers et une certaine optimisation dans l'utilisation des ressources. Par conséquent, le client serait en mesure de connaître les dépenses qu'il aurait à faire en fonction de ses moyens financiers.

4.1.3.4 La gestion des partenariats

Dans les projets réalisés en commun avec des partenaires, il est difficile de signer le protocole d'entente sur les revenus du projet. En effet, les négociations entre l'UQTR et ses partenaires sont souvent difficiles sur le partage des revenus, l'utilisation des subventions, les livrables intermédiaires à produire, etc. De plus, le département des TI de l'UQTR n'a pas le pouvoir d'imposer le respect des échéanciers à ses partenaires.

4.1.3.5 Le respect des droits de propriété intellectuelle

Il faut être sûr de détenir ce qui est légalement permis. Dans les projets de développement de réseaux Internet, il est possible qu'il y ait recours à des images, des sons ou même des articles qui seront introduits dans la technologie. Cela nécessite le respect des droits relatifs à leurs auteurs. Également, il est important de surveiller le respect de ces droits de la part des professeurs et des partenaires du projet. Pour ce faire, l'UQTR fait souvent appel à ses avocats pour examiner le degré de son respect à la question des droits de propriété.

4.1.3.6 L'adhésion des utilisateurs

L'utilisation des réseaux Internet, en particulier l'Intranet représentait pour le personnel de l'UQTR un changement radical dans leurs méthodes de travail. Il s'agit même d'un changement organisationnel pour ces derniers du fait de l'accroissement de la décentralisation. Le risque auquel faisait face le département des TI était le niveau d'acceptation de cette technologie de la part des utilisateurs au sein de l'université. Toutefois, le directeur chargé du développement des SI au sein de l'UQTR, note que le service de l'inscription via Internet fut bien reçu. D'ailleurs, il y eu environ 70% d'étudiants qui l'ont utilisé durant sa première année. Cependant et dans le but de prévenir les erreurs d'utilisation, l'équipe de projet avait intégré des messages affichant des instructions à suivre par les utilisateurs du réseau dans le but d'assurer la bonne utilisation des services offerts.

4.1.4 Commentaires

Ce qui est important à constater en premier lieu c'est que l'UQTR est une institution bien équipée en technologies de l'information lui permettant d'optimiser ses services offerts aux étudiants et d'être même avant-gardiste dans ce domaine à l'échelle provinciale (les inscriptions en ligne). Cela témoigne de l'engagement de la direction de l'université à assurer le bon déroulement de l'activité étudiante dans la région de la Mauricie. L'équipe du département des TI a travaillé en collaboration avec les dirigeants.

Toutefois, nous n'avons pas pu conclure de l'existence d'une politique de gestion du risque proprement dite au sein du département des TI de l'UQTR. Au contraire, le département procède d'une façon réactive quand il entreprend une nouvelle implantation technologique. À l'encontre de ce que préconisait Lanza (2001), la gestion du risque ne fait pas partie du cycle de vie des projets d'informatisation entrepris au sein de l'UQTR. Il revient aussi bien à la direction qu'au département de repenser la politique de gestion du risque qu'ils mènent, et ce, en l'orientant vers plus de prévention et de pro-activité. Cependant, l'UQTR jouit de la présence d'un climat de travail favorisant la créativité. Buttrick (2002) avait en effet mis l'accent sur cet atout dans le but de réussir la politique de gestion du risque. Plus encore, ce dernier a appelé à la nécessité de la valorisation du soutien financier de la part de la direction, chose qui est déjà une réalité à l'UQTR. En effet, tous les projets d'informatisation sont menés jusqu'à la fin sans contraintes financières.

En ce qui concerne les critères ayant contribué au choix de la technologie des réseaux basés sur Internet, la méthode que suit le département repose sur une estimation sommaire des coûts d'implantation, et ce via un devis détaillé des tâches et des dépenses comme l'a avancé Pradels (1981). Cela représente en fait un bon moyen leur permettant d'éviter les investissements dépassant la capacité de l'université. Il est aussi évident que les revenus issus de ces investissements soient plus importants durant l'étude de rentabilité.

L'utilisation des indicateurs de rentabilité des investissements comme la VAN avancée par Mantel et Meredith (2000), n'était pas possible dans le cas des projets de l'UQTR, et ce, en raison de la difficulté dans l'attribution des avantages aux nombreuses politiques de promotion menées en vue de les atteindre. En d'autres termes, l'UQTR fait recours à un certain nombre de politiques qui se combinent dans le seul but d'attirer plus de clientèle à savoir les étudiants. Dans ce cadre, l'acquisition des TI ne représente qu'un aspect de l'ensemble de ces politiques dont il est quasiment impossible de déterminer la contribution exacte au niveau de l'accroissement de la performance de l'Université par la suite.

Quant aux critères relatifs aux orientations stratégiques de l'institution en question, les projets d'informatisation menés par l'UQTR correspondent à la mission de cette dernière dans la

mesure où les apports de ces projets sont examinés au niveau stratégique. Cela témoigne d'un esprit de planification stratégique positif de la part des responsables de l'UQTR tel que confirmé par Chokron (1996) qui pense que la planification stratégique représente une façon d'analyser et de maîtriser les enjeux de la compétition. Également, les alliances stratégiques surtout celles conclues avec d'autres universités s'inscrivent dans le cadre d'une bonne projection stratégique étant donné que les universités sont souvent reconnues pour leur créativité et leur engagement.

Si nous procédons à une analyse des choix technologiques de l'UQTR par rapport aux cinq forces concurrentielles de Porter (2001), nous constaterons que l'implantation de ces réseaux a contribué à l'amélioration de la position concurrentielle de l'UQTR face au reste des universités québécoises et l'affaiblissement du pouvoir de négociation de sa clientèle. Concernant cette deuxième force concurrentielle, Paquin (1990) préconisait que la technologie innovatrice permet à l'entreprise de fidéliser ses clients dans la mesure où ils auront de la difficulté à retrouver certaines caractéristiques clefs de ses produits dans ceux offerts par ses concurrents. Dans ce sens, l'UQTR à travers le service d'inscription en ligne a pu développer un service facile et accessible à ses étudiants qui lui avait permis de renforcer sa position par rapport au reste des universités québécoises.

Cette réussite au niveau de la planification stratégique de l'UQTR suppose nécessairement une bonne gestion de la structure organisationnelle des projets. Dans ce cadre, le département des TI de l'UQTR a fait le bon choix en optant pour la discussion et l'échange, tout en faisant intervenir toutes parties intéressées par le projet (département des TI, professeurs, étudiants, etc.). Cela est de nature à permettre à ces différentes parties d'exprimer leurs opinions concernant leurs rôles et l'organisation du travail, une position qui correspond aux arguments de Marchewka (2003). Cela favorise également l'intégration et l'épanouissement des ressources venant de l'extérieur. Sur un autre plan, le fait que le chef de projet se réserve le pouvoir décisionnel définitif à l'égard de son équipe, permet d'éviter les conflits de directives issues de certaines interventions de la part des directeurs fonctionnels comme l'avançait Buttrick (2002).

Comme nous l'avons signalé au début de cette sous-section, l'UQTR ne dispose pas d'une politique claire dans la gestion du risque. Marchewka (2003) et Feringa et al. (2001) soutiennent

la nécessité de la présence d'un processus auquel l'entreprise a recours d'une façon systématique quand il y a lieu de gérer un risque relatif à l'implantation d'une TI. Plus encore, selon Buttrick (2002), l'absence de processus de gestion du risque peut faire échapper certaines opportunités pouvant avoir des conséquences positives sur le déroulement du projet. Cependant, le département des TI exécute une partie de la première phase du processus de gestion du risque que nous avons adapté dans la figure 2. L'unique activité consiste en la spécification de la technologie. En effet, Feringa et al. (2001) ainsi que McLaughlin (2003) soutiennent que la spécification de la technologie représente la première étape pour réussir le processus de gestion du risque.

Par ailleurs, le reste des phases n'est pas exécuté par le département. La phase 2 du processus est absente dans la mesure ou il n'y a pas lieu de réunions qui se font entre les membres de l'équipe de projet en vue d'identifier les risques avant de procéder à l'implantation du projet. Pareillement, la phase 3 n'est pas exécutée au sein de l'UQTR parce que l'étude des risques ne comporte pas des prévisions quant a l'amplitude et la potée des risques en cas de leur réalisation. De plus, nos répondants ne reconnaissent pas la présence de l'étape 5, à savoir la surveillance du processus de gestion du risque du fait qu'il n'y a aucun rapport d'état qui est produit ni de révisions apportées.

Ainsi, l'absence d'une politique de gestion du risque au sein de l'UQTR explique en quelque sorte la forte présence de risques présentés dans la sous section précédente et que nous catégorisons ainsi :

1. Risque financier : l'adhésion des utilisateurs ; la gestion des partenariats et le respect des droits de propriété intellectuelle ;
2. Risque technique : suivre l'évolution de la technologie ;
3. Risque de coût : la correspondance de la solution adoptée à la capacité de financement du client ; et
4. Risque d'échéancier : la définition du contenu de la technologie[23].

[23] En effet, les révisions souvent apportées au contenu de la technologie entraînent des retards dans la réalisation du projet.

Ces risques et leurs modes de gestion sont venus enrichir certes le contenu théorique de ce travail de recherche surtout ceux relatifs à la gestion des partenariats, le respect des droits de propriété intellectuelle et la correspondance de la solution à la capacité financière du client du projet.

Également, nous avons pu constater que la stratégie de gestion du risque privilégiée par le département des TI de l'UQTR tend vers l'atténuation et le transfert des risques. En ce qui concerne la première stratégie, elle représente une conséquence logique de l'attitude réactive du département face aux risques. Il fallait normalement et compte tenu de la mission et du rôle social de l'UQTR au niveau régional, d'essayer de prévenir ces risques au lieu de les gérer une fois réalisés via le transfert à une autre partie qu'il soit l'assureur ou le sous-traitant. Dans la sous-section suivante, nous présentons certains commentaires concernant l'approche déployée par l'UQTR dans la gestion du risque. Le graphique ci-dessous illustre l'approche de gestion du risque adoptée au sein de l'UQTR.

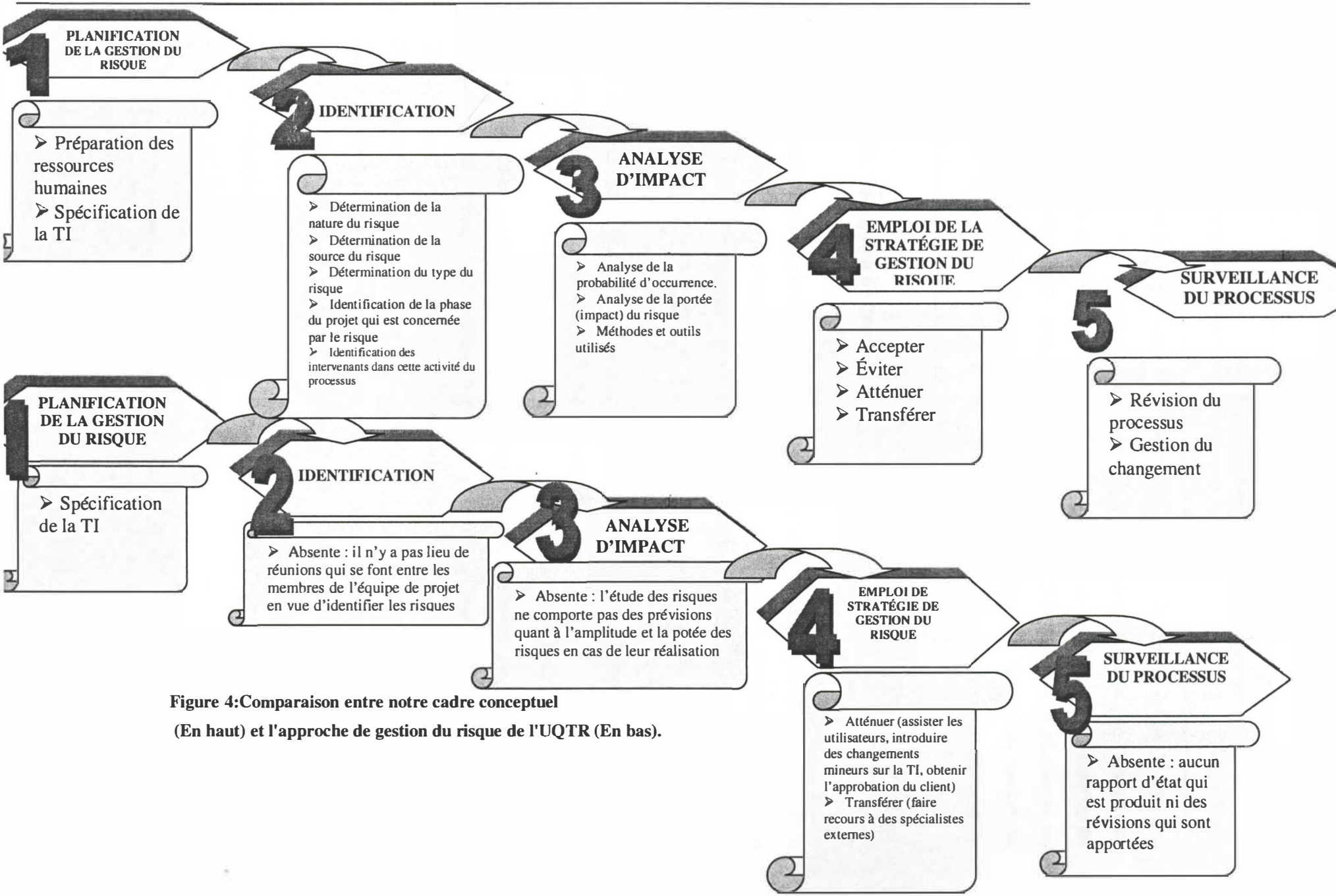


Figure 4:Comparaison entre notre cadre conceptuel

(En haut) et l'approche de gestion du risque de l'UQTR (En bas).

4.2 Cas 2 : Communication Inc[24]

Communication Inc. représente une entreprise qui s'appuie fortement sur les TI dans son activité. En effet, le secteur dans lequel opère cette firme se caractérise par l'importante contribution de la technologie dans l'amélioration de la qualité des produits offerts aux clients. Il devient indispensable pour Communication Inc. de bien exploiter ces technologies et les mettre à profit. Pour ce faire, nous verrons dans ce qui suit une brève description de l'entreprise et de son secteur d'activité, ses principales TI et nous observerons l'approche de gestion du risque mise en application par la firme.

4.2.1 La description de l'entreprise

La deuxième entreprise étudiée dans ce travail de recherche oeuvre dans le secteur de la communication et du marketing. Située dans la ville de Montréal, Communication Inc. a débuté modestement en employant seulement une dizaine de personnes. À son départ, en 1982, Communication Inc. vivait seulement de petits contrats locaux. Elle s'est spécialisée dans la publicité, le marketing et la consultation. Qui plus est, elle offre ses services dans d'autres domaines connexes à la communication et à la gestion. À la fin d'avril 2002, Communication Inc. possèdait d'autres succursales à Québec et à Ottawa.

La structure organisationnelle de l'entreprise Communication Inc. se définit par la formation d'un conseil d'administration dont un président et plusieurs vice-présidents. Les vice-présidents sont répartis dans divers départements. L'effectif de Communication Inc. s'élevait à 125 employés ayant plusieurs années d'expérience en gestion de commandites et en marketing événementiel. De plus, elle est reconnue pour sa minutie et son efficacité sur le terrain, notamment douée pour la logistique, et elle s'engage au maximum dans tous ses dossiers. Ainsi et au fil des années, Communication Inc. a pris de la notoriété. La plupart des contrats octroyés à Communication Inc. dans les dix dernières années provenaient essentiellement du niveau national ou international.

---

[24] Le vrai nom de la compagnie n'est pas dévoilé dans ce travail de recherche pour des considérations de confidentialité exprimées par les dirigeants de la compagnie. Pour les fins de ce travail, nous utiliserons « Communication Inc. »

Par conséquent, son expertise était largement reconnue à l'échelle nationale. Désireux de satisfaire les besoins des clients en matière de gestion et d'exploitation de commandites et d'activités promotionnelles, Communication Inc. appuyait sa clientèle dans l'atteinte de leurs objectifs et de leurs réalisations. Pour ce faire, l'équipe de Communication Inc. aide les clients dans les sphères spécifiques allant de la consultation stratégique à la direction artistique et de la rédaction à la production. Ainsi, la compagnie avant 2002 figurait parmi les grands dans les domaines de la communication, du marketing et de la consultation au Québec.

Au Canada, il y a un peu plus d'une centaine d'entreprises listées dans les mêmes domaines que Communication Inc. De ce nombre, environ trente-cinq œuvrent au Québec. Les milieux de la publicité et du marketing sont des secteurs d'activités qui se caractérisent par une forte compétition. En effet, la concurrence impitoyable et les guerres politiques ont mené au démantèlement partiel de l'entreprise. Les informations contenues dans les sous-sections suivantes on été puisées à partir d'une entrevue réalisée avec l'ex-directrice du département des TI de Communication Inc. Ainsi, nous parlerons des apports des TI pour la compagnie et nous présenterons les méthodes qu'elle déploie pour la gestion du risque inhérent à ces technologies. Enfin, nous formulons une série de commentaires sur la politique de gestion du risque de Communication Inc.

4.2.2 Les principales TI et leur place dans l'organisation

Communication Inc. dispose d'un réseau interne basé sur la technologie client/serveur lui permettant d'échanger des informations entre ses employés. En effet, la technologie client/serveur a permis à Communication Inc. d'augmenter sa compétitivité en donnant à ses employés le moyen de mieux réagir et répondre aux besoins de son marché. Ceci est rendu possible grâce à une meilleure répartition de l'information et de traitements appropriés sur l'ensemble du réseau reliant les postes de travail des utilisateurs. Concrètement, tout système client/serveur comprend un certain nombre d'ordinateurs, de systèmes d'exploitation, d'applications et de données reliés entre eux, permettant ainsi de fournir les informations les plus récentes, très rapidement et sous la forme requise par l'utilisateur. Sur un autre plan,

Communication Inc. a recours à un ensemble de logiciels avancés dans son activité pour bien assurer les tâches de marketing et de consultation qu'elle exécute. Dans ce cadre, certains clients de la compagnie pouvaient aller chercher des documents à partir de ce réseau.

En plus de la technologie du client/serveur, Communication Inc. est connectée au réseau Internet. En effet, tous les postes dans la compagnie sont reliés à Internet qui représente leur première source au niveau de l'obtention des informations sur le marché, l'actualité, les concurrents, etc. De plus, les employés de Communication Inc. ont accès à des courriers électroniques à l'adresse de la compagnie. Ils disposent d'une grande capacité de stockage leur permettant de recevoir et d'envoyer des fichiers de grande taille. Il s'agit d'un moyen privilégié au sein de Communication Inc. pour le transfert des fichiers.

Il y avait un projet d'installation d'un Intranet en cours de conception pour des fins d'accélération de la production au niveau des filiales de Communication Inc. De plus, elle comptait utiliser une telle technologie avancée pour mieux gérer ses contrats avec ses clients installés à l'extérieur. Toutefois, ce projet n'a pas été achevé en raison du démantèlement partiel de la firme. Comme nous venons de le voir, Communication Inc. est bien équipée en termes de TI. Cela nous amène alors à s'interroger dans la sous-section suivante sur l'amplitude des risques qu'elle rencontre durant l'implantation de TI ainsi que sur l'approche qu'elle utilise en vue de les contrer.

4.2.3 Les risques relatifs aux réseaux basés sur Internet et leurs modes de gestion

Pour les dirigeants de Communication Inc., les technologies de l'information représentent l'outil par excellence en ce qui concerne une entreprise qui travaille dans la communication. Il s'agit pour eux de leur premier atout dans leur activité. Les apports des TI se situent pour Communication Inc. au niveau de l'accès à l'information. Les employés de la compagnie sont constamment au courant de ce qui se passe sur le marché à l'aide des outils que leur offrent les réseaux Internet. De plus, ces derniers leur permettaient de connaître les innovations technologiques qui émergent et de les acquérir dans le but d'améliorer les processus d'affaires.

Au début, la direction n'était pas assez consciente des apports de ces réseaux. Toutefois et au fil du temps, elle a pu constater par elle-même la grande contribution qu'avait cette technologie au niveau de l'amélioration du rendement de ses employés surtout dans un secteur d'activité aussi dynamique que la communication et le marketing. La direction a même engagé des ressources dans le cadre du support technique à ses réseaux. De même, elle a fait appel aux services d'une firme spécialisée dans le maintien et l'entretien des réseaux des entreprises. Également, Communication Inc. faisait recours à des ressources externes durant les projets de développement d'applications logicielles.

Actuellement, la firme acquiert toutes les innovations technologiques. Plus encore, les serveurs ont été remplacés afin qu'ils soient plus puissants et la qualité de la connexion à Internet a été améliorée. Ce changement de mentalité a été induit par les efforts du département des TI de Communication Inc. En effet, ce dernier a tenté à travers une série de rencontres avec les dirigeants de la firme – en particulier le directeur financier – de démontrer l'utilité de ces technologies et leurs effets sur la rentabilité et l'image de marque de la compagnie.

Les dirigeants n'étaient pas motivés au début à dépenser des sommes énormes dans l'installation de ces réseaux surtout par crainte des échecs qui sont survenus chez certains concurrents au niveau international tels que les attaques, les intrusions et les virus. De ce fait, ils craignaient la perte de rentabilité et la sécurité de ces réseaux Internet surtout au moment de l'échange de documents confidentiels avec certains clients ou même entre les employés.

Concernant le choix des réseaux Internet, le principal critère était la correspondance aux besoins de la firme relativement à la rapidité d'exécution. Par exemple, à l'aide d'Internet Communication Inc. avait la possibilité de transférer du son et des images, ce qui n'étaient pas aussi rapide avec le courrier traditionnel. Cela lui a permis effectivement de réduire ses coûts d'opération. Par contre, l'étude de rentabilité concernait seulement le niveau de satisfaction des utilisateurs par rapport à la rapidité d'exécution des tâches. Dans ce cadre, la ressource interviewée affirme que les employés de Communication Inc sont tellement bien rémunérés que les minutes perdues dans leur travail risquent de coûter très cher à la firme. Par conséquent, il était facile et évident de constater la contribution des réseaux de communication

en particulier les réseaux Internet au niveau de la rapidité d'exécution des utilisateurs. Ainsi, malgré les coûts importants associés à son implantation, les bénéfices rattachés aux réseaux Internet étaient importants.

Au niveau de la contribution des réseaux Internet par rapport à la mission de l'organisation, le département des TI était conscient des apports au niveau stratégique de cette technologie. Les employés avaient constaté par eux-mêmes la différence au niveau de leurs méthodes de travail et cela a eu des effets sur leur rendement. Ces réseaux ont même amélioré la position de Communication Inc. sur le marché par rapport à ses concurrents. Certes, la technologie avait coûté plus cher que pour d'autres entreprises mais la qualité des services offerts était nettement meilleure que ce que faisait la firme antérieurement. En effet, la répondante affirme que Communication Inc. était supérieure à ses nombreux concurrents au niveau de ses installations technologiques et qu'il était facile pour les clients de constater cette réalité au niveau des services.

En ce qui a trait à l'organisation du travail au niveau du département des TI, il est à noter qu'il y avait des ressources qui venaient de l'extérieur pour soutenir le travail du département, et ce, de façon contractuelle. Dans le but de bien s'organiser, les rencontres entre ces différents intervenants étaient multiples et fréquentes afin de surmonter certains problèmes techniques au niveau du réseau souvent soulevés par les utilisateurs. S'il s'agit de problèmes sérieux, il y a lieu alors de les transférer à des spécialistes externes. Toutefois, les techniciens de la compagnie étaient dans la plupart du temps en mesure de régler ces problèmes. En effet, la répondante affirme que l'ambiance de travail au sein de l'équipe du département favorisait la qualité et la rapidité de la réponse aux problèmes, et ce, malgré la pression exercée parfois de la part de certains utilisateurs. Cela nous amène à s'interroger sur la nature des risques auxquels fait face le département des TI de Communication Inc.

Dans ce cadre, notre répondante ramène la majorité des risques qu'elle rencontrait à la question de la sécurité des réseaux Internet. Pour elle, le processus de gestion du risque doit s'exécuter sur une base quotidienne dans le cadre d'une politique de prévention bien élaborée, et ce, afin d'éviter les répercussions de tels risques. L'autre catégorie de risque se rapporte au

manque de collaboration des utilisateurs de cette technologie. La répondante soutient la stratégie d'évitement (politique de prévention) et de transfert (spécialistes et assurance) dans sa réponse aux risques. Dans les paragraphes qui suivent, nous explicitons davantage la nature de ces risques ainsi que l'approche à laquelle se fie Communication Inc. dans sa politique de gestion du risque.

4.2.3.1 La sécurité du réseau

Le principal risque auquel faisait face le département des TI de Communication Inc. est le risque de sécurité du réseau Internet. En effet, certains risques relatifs au dommage des virus, aux intrusions, etc. représentaient des menaces constantes qu'ils fallaient contrer d'une façon régulière. Par conséquent, l'équipe du département avait opté pour l'approche proactive en mettant en place un processus de gestion du risque exécuté quotidiennement et comportant un ensemble de tâches visant la sécurité de l'utilisation de toutes les installations technologiques dans la compagnie et la préservation de la confidentialité des données. Ainsi, le département procédait à une vérification quotidienne et fréquente des fonctionnalités des serveurs, des entrées et des sorties, du fonctionnement des courriers électroniques, des logiciels, etc.

Il y avait même une personne du département dont la tâche consistait à identifier les nouveaux outils et applications permettant d'assurer la sécurité du réseau. Également, l'équipe observe les problèmes que rencontrent d'autres entreprises dans le cadre de l'exploitation de leurs réseaux Internet. Ainsi, l'équipe est en mesure de constater les graves conséquences que peuvent avoir de telles défaillances sur le fonctionnement et la rentabilité de la firme. Sur un autre plan, les serveurs sont très développés et extrêmement sécuritaires. Par exemple, le système bloque automatiquement lorsque l'activité de téléchargement dépasse la normale. Ainsi, la direction avait choisi de miser sur des investissements importants pour plus de sécurité. Sur un autre plan, l'équipe du département procédait à la documentation des risques s'ils sont réalisés en vue de les prévenir dans l'avenir. Plus encore, le département avait opté pour l'assurance de ses réseaux contre les risques de vol, d'incendie, de dégâts d'eaux, etc.

Par ailleurs, une telle politique de prévention ne peut être efficace que si elle est soutenue par la collaboration des utilisateurs, chose qui n'était pas présente dans le cas de Communication Inc. Dans la sous-section suivante, nous mettons la lumière sur le manque de collaboration de certains intervenants dans le cadre des réseaux Internet.

4.2.3.2 La collaboration des utilisateurs

Le département avait défini une politique visant une utilisation adéquate et non abusive des réseaux Internet de la compagnie. Selon l'interviewée, cette politique s'adressait aux employés et au reste des utilisateurs externes de la technologie. Cette politique était établie sur la base des problèmes connus par d'autres entreprises ayant opté pour la même technologie et qui ont abouti même à la disparition de ces dernières. Malheureusement, la répondante déplore le manque de respect de certains utilisateurs des procédures mises en place. En effet, certains utilisateurs abusent du réseau en contournant les instructions, ce qui cause certaines défectuosités. Malgré leurs actions dommageables pour la compagnie, ces utilisateurs demandent au département d'apporter des solutions immédiates à leurs problèmes en exerçant de la pression.

Plus encore, ces utilisateurs sont peu coopératifs quand le département tentait de solliciter leur aide pour le bon fonctionnement des technologies mises en place. En vue de contrer ce manque de collaboration et ce manque de respect des procédures, le département des TI de Communication Inc a choisi d'aller chercher plus de soutien de la part de la direction qui n'a pas manqué d'en fournir.

De plus, l'équipe du département avait souvent réagi avec beaucoup de patience et avait réglé à temps les défaillances et les erreurs. Dans le paragraphe suivant, nous commentons l'ensemble des méthodes de gestion du risque déployées par Communication Inc. et nous schématisons cette approche à l'aide de l'illustration graphique présentée au deuxième chapitre de ce travail de recherche.

4.2.4 Commentaires

Si nous avons à formuler une interprétation générale des conclusions tirées à partir de l'entrevue réalisée avec l'ex-directrice du département des TI de Communication Inc., ce serait que la politique de gestion du risque de Communication Inc. est presque conforme à ce qui a été avancé dans la partie théorique de ce travail de recherche. En effet, nous verrons tout au long de cette sous-section le degré de conformité de l'approche adoptée par Communication Inc. par rapport aux postulats théoriques présentés par les auteurs que nous avons étudiés.

En premier lieu, nous traiterons la présence des facteurs clefs de succès de la gestion du risque. En ce qui concerne le soutien de la direction, cet élément ne se faisait pas sentir au début. Toutefois, c'est grâce aux efforts des responsables du département des TI qu'il s'est concrétisé. Nous soulignons dans ce cadre la compréhension et l'attitude positive de la direction de la compagnie qui s'est rendue compte de l'importance et de la contribution des TI au niveau de son fonctionnement. Ce changement positif a favorisé les investissements consistant en l'implantation de technologies sophistiquées, ce qui a permis à Communication Inc. de se démarquer de la concurrence. De plus, une telle attitude était à l'origine du bon climat de travail qui s'est instauré au niveau de l'équipe du département des TI. En effet, cela était induit par l'esprit de confiance et d'échanges suscité par la direction.

En ce qui a trait aux critères ayant contribué au choix de la technologie Internet, l'étude de rentabilité n'a pas inclus le calcul des coûts de l'investissement et l'estimation des revenus. Au contraire, elle s'est limitée à une évaluation qualitative des avantages au niveau de la rapidité d'exécution et de leur impact sur la satisfaction des utilisateurs. En effet, il fallait opter pour une étude de rentabilité plus développée telle que soutenue par Mantel et Meredith (2000), Pradels (1981) et ARTE (1986).

Au niveau du deuxième critère relatif à l'ajustement de la technologie à la stratégie de la firme, il est à noter que les dirigeants de la compagnie ont compris que le recours à la technologie Internet allait leur permettre de se repositionner sur le marché et d'affirmer leur

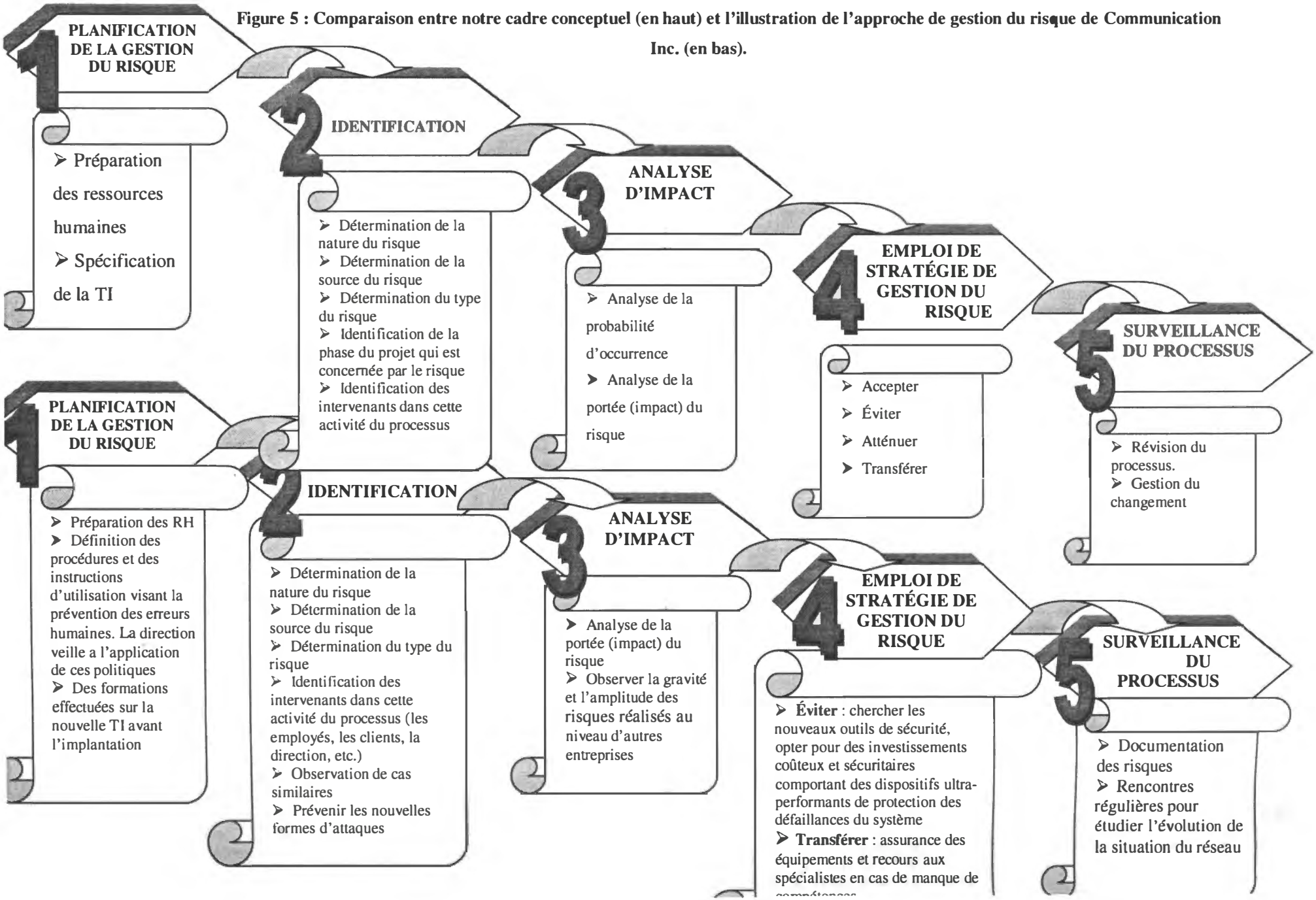
orientation stratégique en améliorant considérablement les méthodes de travail des employés et en facilitant l'accès à l'information.

Quant à la gestion de la structure d'organisation dans le contexte des projets de développement d'Internet, Communication Inc. misait sur la qualité des relations professionnelles dans la mesure où ils bénéficiaient d'un bon climat de travail. Cette bonne organisation a eu un effet positif sur la réduction du temps de réponse aux problèmes.

Ainsi, nous sommes en mesure de constater la présence plus ou moins affirmée des facteurs clefs de succès à la gestion du risque. Cela nous amène à mettre en évidence la politique de gestion du risque de Communication Inc. Dans ce cadre, nous signalons la présence d'un processus de gestion du risque entretenu de façon quotidienne. Par conséquent, nous concluons quant à la nature de la réponse proactive déployée par Communication Inc. Au niveau de la phase de planification, il y a une bonne préparation des ressources humaines à travers la mise en place d'un certain nombre d'instructions et de procédures visant la prévention des erreurs humaines telle que préconisée par Greenstein et Vasarhelyi (2002). Par contre, l'équipe du département des TI ne procède pas à la spécification de sa technologie (Feringa et al, 2001).

Quant à la phase d'identification des risques, nous avons noté la présence d'une ressource chargée d'identifier les nouvelles formes d'attaques des réseaux mis en place. Également, les observations de certaines situations délicates qu'ont connues des entreprises ayant échoué l'implantation de la même technologie, représente un moyen efficace et privilégié pour Communication Inc. dans l'identification des menaces possibles à son réseau de communication. Plus encore, les vérifications fréquentes de la qualité des installations technologiques s'inscrivent aussi dans ce cadre. Dans l'adaptation graphique ci-dessous de l'illustration que nous avons conçue au deuxième chapitre, nous récapitulons l'application du processus de gestion du risque assurée par Communication Inc.

Figure 5 : Comparaison entre notre cadre conceptuel (en haut) et l'illustration de l'approche de gestion du risque de Communication Inc. (en bas).



4.3 Cas 3 : Telus Solutions d'affaires

4.3.1 La description de l'entreprise

Telus Solutions d'affaires représente une filiale de l'entreprise de télécommunication canadienne Telus Corporation qui compte plus de 26000 employés partout au Canada. En effet, cette dernière se compose de deux principales filiales à savoir Telus Mobilité qui oeuvre dans le domaine de la téléphonie et qui occupe notamment le premier rang des entreprises de communication sans fil au Canada et Telus Solutions d'affaires qui propose de nouveaux concepts stratégiques selon les processus d'affaires de ses clients au Québec. C'est dans le cadre de la deuxième filiale que s'inscrit cette troisième étude de cas relative à notre travail de recherche. La firme Telus Solutions d'affaires a été fondée en 2000 par Telus Québec qui désirait, à travers la création de cette filiale, élargir la gamme de ses produits vers des solutions d'affaires électroniques s'adressant à sa clientèle au Québec. Les services qu'offre Telus Solutions d'affaires[25] se rapportent au développement des concepts suivants[26]:

- Cybermarketing ;
- Intelligence des affaires (veille stratégique) qui consiste à fournir une base pour soutenir la prise de décisions bien fondées de la part des dirigeants des entreprises (recensement de données sur le marché et la concurrence, diagnostic interne et externe et gestion de la masse informationnelle) ;
- Progiciels de gestion intégrée (ERP: Entreprise Resource Planning) ;
- Gestion de la relation client (CRM: Customer Relationship Management) ;
- Communication Web ;
- Portails et places d'affaires électroniques ;
- Intranets et Extranets ;
- Systèmes nomades ;
- Sécurité et infrastructure.

---

[25] Nous nous contenterons de l'appellation Telus puisqu'il s'agit de la même politique pour l'ensemble des filiales de la compagnie Telus Corp.

[26] Source : http://www.telussolutionsdaffaires.com/solutions/solutions.jsp

L'ensemble de ces services supporte les clients de Telus Solutions d'affaires dans l'atteinte de leurs objectifs surtout sur le plan stratégique. Les projets que réalise la compagnie sont parfois d'une grande envergure et demandent la participation de plusieurs équipes multidisciplinaires. Dans ce cadre, Telus bénéficie de l'existence d'une infrastructure de communication pan-canadienne et compte également sur une panoplie d'expertises qu'elle regroupe parmi son effectif. En effet, ces expertises se rapportent à la gestion stratégique (gestion des processus et organisation du travail, gestion des connaissances et des compétences, gestion des TI et gestion des opportunités et des risques), la conception et l'architecture (design graphique, style et normes de rédaction, ergonomie), développement de solutions logicielles (client-serveur, système central, environnement Web, etc.), déploiement et migration (aider les organisations à mieux gérer les changements au niveau de la technologie utilisée), l'exploitation et l'impartition (la prise en charge des tâches d'entretien des infrastructures technologiques afin que le client puisse se consacrer sur sa mission centrale).

C'est pour cette raison que le recours à Telus dans le cadre de la partie empirique de notre travail de recherche se révèle très utile. En effet, l'entreprise répondante exploite et développe en même temps des outils de communication basés sur la technologie Internet. Cela serait de nature à bien fonder les arguments qui en étaient collectés à partir de l'entrevue que nous avons effectuée avec le directeur principal chez Telus. Ainsi, les informations divulguées par notre répondant seront présentées successivement dans les parties suivantes. Dans ce sens, nous présenterons les principales TI dont dispose Telus. Puis, nous mettons la lumière sur les principaux risques auxquels l'entreprise répondante fait face dans son activité ainsi que la méthode de gestion du risque qu'elle déploie pour les contrer. Dans la dernière section, nous formulons nos commentaires relativement à la politique de gestion du risque de Telus.

4.3.2 Les principales TI et leur place dans l'organisation

Les TI représentent l'épine dorsale de Telus. Elles sont utilisées aussi bien à l'interne qu'à l'externe de l'organisation. Ces technologies se rapportent à la téléphonie et aux réseaux informatiques, aux applications de support à la clientèle et aux logiciels s'adressant au personnel qui est au service de la clientèle. Ces applications s'appuient entre autres sur un site Web, un

Intranet et la technologie « One Source » qui consiste en un guichet unique disponible à tous les employés de Telus. Les TI ont facilité et amélioré selon le répondant la communication interne chez Telus qui dispose d'un effectif de 26000 employés au Canada comme c'est déjà noté ci-haut.

Le président de la filiale réalise hebdomadairement des mémos à l'attention des employés. Selon la ressource interviewée, cela est de nature à renforcer la culture d'entreprise auprès du personnel et permet sur un autre plan d'optimiser la gestion de la gigantesque masse informationnelle qui représente le champ d'action principal de Telus. La performance de certaines ressources de Telus est communiquée au reste des employés, et ce, dans l'objectif de susciter de l'engagement et de la motivation auprès de ces derniers. Par ailleurs, les employés à la retraite sont en mesure de garder le contact avec leur compagnie qui aura fort probablement besoin de leur soutien et expérience ultérieurement.

La technologie de vidéoconférence et d'Internet est très utilisée chez Telus. Ainsi, les interférents n'ont plus besoin d'être présents physiquement. Pour mettre en place l'ensemble de ces technologies avancées, Telus a dû investir des millions de dollars pour étendre les réseaux de communication à toutes les régions du pays. Elle développe les infrastructures par ses propres moyens. Ces réseaux s'adressent aussi bien aux employés qu'aux clients et ce partout au Canada. C'est ainsi que les dirigeants de la compagnie soutiennent que l'importance relative des investissements en infrastructure technologique est négligeable face aux impératifs de pérennité de l'entreprise.

4.3.3 Les risques relatifs aux réseaux basés sur Internet et leurs modes de gestion

En raison de la nature de sa mission qui consiste dans l'offre de solutions électroniques développées à ses clients. Telus n'a pas le choix que de tenter constamment d'acquérir toutes les innovations technologiques sur le marché. Il serait par conséquent évident de supposer l'existence d'une grande volonté de la part de la direction de la compagnie à soutenir cette tendance et à la renforcer. C'est ainsi que la direction de Telus est toujours à l'écoute des attentes de ses employés et de leurs besoins. De plus, Telus offre la même technologie à ses clients s'il se révèle qu'elle est

efficace à l'interne. Par conséquent, la direction est appelée à veiller sur l'acquisition des technologies qui soient vraiment performantes et soutiennent le fonctionnement de la compagnie.

Lors du choix des technologies à implanter, Telus se fie à sa réputation positive. Dans ce sens, il importe que la technologie soit reconnue comme étant un standard dont l'efficacité a été déjà prouvée ailleurs auprès d'autres entreprises. Parfois, ces technologies sont expérimentées à l'interne avant de les offrir aux clients. Il s'agit de critères portant en général sur la qualité de l'innovation en question. Ce choix s'impose en raison de l'importance des réseaux de la compagnie auxquels la technologie est destinée.

Par ailleurs, il y a recours à des études de rentabilité basées sur des dossiers d'affaires ou des « business cases » très raffinés. Ces études consistent en des grilles d'analyse et des méthodes standard permettant d'évaluer le rendement des investissements de Telus. Les gabarits doivent être appliqués à tout projet avant qu'il soit entrepris, et ce, afin de déterminer les avantages, les inconvénients ainsi que les risques afférents. Il s'agit pour les dirigeants de la compagnie d'une exigence ayant des répercussions positives sur la rentabilité des investissements.

Sur le plan stratégique, les apports du réseau au niveau stratégique sont observés avec rigueur, et ce, tout en ayant regard aux valeurs corporatives de l'organisation. Dans ce cadre, les évaluateurs élaborent un pointage pour vérifier le degré d'atteinte de chaque valeur pour décider la pertinence stratégique d'un l'investissement. Il est à noter que l'Est du Canada (Québec et Ontario) représente un marché émergeant pour Telus étant donné que la compagnie détient de bonnes parts du marché dans l'Ouest. Dans ce cadre, les investissements déjà effectués ont eu une contribution incontestable d'atteinte d'une plus grande part de marché.

En ce qui concerne le travail au sein des équipes de projet, Telus fait souvent recours à des ressources de l'extérieur en particulier des consultants spécialisés. Ces ressources sont bien intégrées selon notre interviewé dans les équipes de projet. Ce dernier juge que la communication est fluide avec les consultants. De plus, Telus procède toujours après clarification du mandat, ce qui permet d'éviter toute confusion ou conflit par la suite. Cela nous introduit à la présentation des risques auxquels fait face Telus Solutions d'affaires. En effet, le premier risque concerne

notamment la participation de ressources externes aux projets que réalise la compagnie, nécessitait une gestion des différences notamment celles d'ordre culturel. Quant au deuxième risque, il porte sur la gestion des changements imprévisibles qui surviennent durant l'avancement du projet. Nous présenterons également l'approche de gestion du risque qu'utilise Telus et qui repose sur un ensemble de principes et de standards appliqués à tous ses projets. Cette approche sera détaillée davantage dans les sections qui suivent.

4.3.3.1 La gestion des différences culturelles

Dans l'entrevue effectuée avec le directeur principal de Telus, le répondant avait évoqué un exemple de projet que Telus avait mené pour le profit du gouvernement tunisien et qui consiste dans l'informatisation de la base de données de la caisse nationale de sécurité sociale. L'interviewé avait soulevé la question des différences culturelles dans ce genre de projets qui impliquent le travail en collaboration avec des ressources de plusieurs provenances et ayant des profils et des cultures différentes.

L'équipe qui travaillait sur le projet comportait plusieurs nationalités. Notre répondant qui dirigeait le projet était appelé à harmoniser cette mosaïque de cultures. Certes, les méthodes de travail auxquels les Tunisiens font recours diffèrent totalement de celles déployées en Amérique du Nord et en particulier au Québec. Par exemple, les affaires en Tunisie fonctionnent avec plus de verbal et d'arrangements portant sur l'échange mutuel de services.

Ainsi, l'équipe de Telus avait fait face à cette spécificité de l'environnement dans lequel opère les entreprises tunisiennes dans le sens où elle a eu de la difficulté à faire accepter l'architecture du site Web qui avait été conçue selon la meilleure correspondance aux besoins du client. Le concept tel que défini par Telus comportait le recours à certains logiciels avancés mais coûteux. Cela avait posé des problèmes pour leurs homologues tunisiens qui avaient essayé d'avoir des faveurs relatives au prix. Finalement, le concept a été développé et implanté selon la vision de Telus. L'interviewé nous a confié que le client Tunisien était persuadé en fin de compte de l'utilité de la rigueur de Telus quant aux détails du livrable avant le commencement du projet, et ce dans le but d'éviter les retards. Ces retards sont souvent occasionnés par les négociations

ultérieures relativement à l'augmentation du prix demandé en raison des changements qui doivent être apportés au concept initialement développé.

Également, dans les projets qu'exécute Telus, l'accent est toujours mis sur la nécessité des rencontres régulières et fréquentes entre les participants au projet et en particulier entre les membres de l'équipe qui se charge de l'exécution. Notre répondant disait qu'il n'y avait pas de salles de réunions pour discuter de l'état du projet étant donné que les dirigeants de la Caisse de Sécurité Sociale de Tunisie ne trouvent pas l'utilité de ces rencontres tant que le projet avance selon les attentes. Par conséquent, les représentants de Telus ont dû insister pour aménager une salle spéciale pour les rencontres à toutes les semaines dans l'objectif d'échanger les idées et d'optimiser le fonctionnement du projet. Dans ce cadre, les employés de Telus partent de la conviction qu'en échangeant les visions, ils seront en mesure d'améliorer leur performance même si tout marche comme prévu. Cependant, il est difficile de tout prévoir dans un projet. Il existe toujours des imprévus qui présentent des défis à gérer de la façon la plus efficace. C'est dans ce sens que s'ajoute le deuxième risque que rencontre souvent les équipes de Telus et qui se rapporte à la gestion des changements.

4.3.3.2 La gestion des changements durant le projet

Il s'agit du principal risque souvent rencontré par Telus. Il s'agit des nouvelles circonstances qui s'imposent et qui demandent une certaine faculté d'adaptation de la part de l'équipe de projet. Ce sont des périodes d'inertie qui concernent généralement l'attente des approbations à chaque phase du projet et les objections de la part de certains intervenants. Devant l'éminence de telles menaces, le choix d'une politique appropriée de gestion du risque s'impose pour Telus. Dans ce cadre, la compagnie fait recours à un processus de gestion du risque certifié ISO 9001/2000. Il s'agit de la méthodologie ProMax qui respecte les normes telles que dictées par le Project Management Institute. La méthodologie Promax comporte un suivi mensuel des risques pour tous les projets et repose sur un certain nombre de principes à savoir l'obtention des approbations du client pour chaque étape du projet, la clarification exhaustive des rôles et des responsabilités dès

le début du projet et le contrôle de la qualité des livrables intermédiaires. Elle énonce également six étapes pour le bon déroulement du projet et qui sont les suivantes[27] :

1. **L'engagement**: consiste à détailler le mandat selon les exigences du client. Un estimé des détails du livrable et des coûts est présenté au client avant le commencement du projet, le but recherché étant de garantir l'engagement irréversible du client.
2. **La prise en charge du projet** : le chargé du projet et son équipe effectuent une série de rencontres avec le client dans le but de préciser les attentes des deux parties, l'étendue des travaux, les échéanciers, les risques, les facteurs clefs de succès et les niveaux d'approbation. Le projet démarre au terme de cette étape.
3. **L'ingénierie de la solution** : Il s'agit de concevoir une solution selon le mandat convenu y compris la spécification détaillée de la réponse.
4. **La mise en oeuvre** : elle consiste dans la réalisation de la solution. Des révisions et des corrections peuvent être apportées au concept durant cette étape.
5. **La mise en service** : la livraison finale au client de la technologie développée.
6. **La satisfaction continue** : organiser des rencontres avec le client pour s'assurer de sa maîtrise de la solution et de l'ensemble de ses fonctionnalités, pour garantir la satisfaction de ce dernier dans son utilisation et pour établir la correspondance au mandat de départ.

Par ailleurs, le chargé de projet est tenu de faire rapport de son projet à tous les mois devant le bureau de projets. Il s'agit d'une unité mise en place par Telus qui est responsable de l'application du processus présenté ci haut. Le bureau de projet se compose notamment de plusieurs spécialistes en gestion de projet. Le chargé de projet est appelé à remplir des formulaires sur les risques qu'il identifie ainsi que les méthodes qu'il propose en vue de les mitiger. L'amplitude des risques est mesurée à l'aide d'indicateurs prédéfinis dans un tableau de bord. Dans ce cadre, les impacts des risques sont mesurés, quantitativement et qualitativement, par rapport au rendement financier du projet, à l'image corporative, à la productivité du personnel, etc. Les projets sont retransmis sur MS Project afin de surveiller leur état d'avancement. Dans ce cadre, il y a lieu de vérifier le respect des échéanciers, les dépenses

[27] Source : http://www.telussolutionsdaffaires.com/entreprise/promax.jsp

occasionnées, les états financiers, etc. Par conséquent, les dirigeants de Telus estiment qu'à l'aide de ces outils, tout dérapage dans le projet ne peut dépasser un mois de temps.

Seul le chargé de projet est responsable de l'identification des risques et de les présenter au bureau de projets. Avant le commencement du projet, ce dernier est appelé à remplir le manuel de gestion de projet disponible chez Telus et de l'adresser au bureau de projets afin d'être validé et approuvé. Par la suite, les membres du bureau examinent le contenu du manuel rempli et demandent des éclaircissements de la part du chargé du projet. Les membres du bureau disposent d'une expérience riche dans le domaine spécifique du projet en question leur permettant ainsi de bien fonder leur jugement en ce qui concerne les risques identifiés, leur impact ainsi que les méthodes destinées à leur mitigation proposées par le chargé du projet. Ce dernier peut discuter avec le client lors de l'élaboration de son rapport. Il existe des tables d'utilisateurs sélectionnés pour en récolter les perceptions face à l'approche proposée. Une personne hiérarchiquement plus élevée peut même entrer en contact avec le client afin de trouver la solution appropriée selon ses attentes. Parfois, Telus fait appel aux couvertures d'assurance et aux sous-traitants dans le cadre de certains projets d'envergure. La prochaine section présentera l'approche de gestion du risque mise en oeuvre par Telus, et ce, par rapports aux énoncés théoriques de ce travail de recherche.

4.3.4 Commentaires

D'après les informations collectées sur la politique de gestion du risque de Telus, il est clair que l'approche déployée est très standardisée. En effet, elle s'applique avec rigueur à tous les projets entrepris par la compagnie. Certes, cette politique s'appuie sur les recommandations du Project Management Institute[28] qui est un organisme mondialement reconnu et regroupant des gestionnaires de projet de partout dans le monde. Dans les paragraphes qui suivent, nous commentons l'ensemble des éléments qui composent l'approche de gestion du risque de Telus.

En ce qui concerne le soutien de la direction, il s'agit d'un appui illimité aux efforts d'acquisition des nouvelles technologies et de les offrir dans un premier temps aux employés puis

[28] www.pmi.org

aux clients lorsque l'efficacité de la TI est confirmée. Une telle position positive de la part de la direction est soutenue par la mission même de Telus, qui est d'offrir des technologies ultra développées à ses clients en vue de soutenir leurs processus d'affaires. De plus, il est à noter la forte concurrence à laquelle fait face la compagnie à l'échelle nationale, ce qui porte l'attention de Telus sur l'anticipation des besoins de sa clientèle.

Par ailleurs, nous soulignons la conscience de la direction des apports des TI au niveau du renforcement de la culture d'entreprise, et ce, à travers la facilitation des modes de communication entre les différents départements et échelons de la compagnie. Cela améliore le climat de travail et représente sans doute un facteur concourant à l'amélioration de la rentabilité de Telus.

Quant aux critères de choix des TI, ils reposent essentiellement sur la qualité démontrée, qu'elle soit à l'interne ou auprès d'autres compagnies les ayant déjà implantées. Il s'agit en fait d'un choix imposé par l'envergure des investissements à mettre en place, et ce, par rapport à l'étendue du marché canadien à couvrir. Par ailleurs, les études de rentabilité que réalise Telus dans le cadre de ses projets sont assez poussées et permettent en conséquence de bien élaborer les prévisions des coûts et des bénéfices attachés et d'éviter ainsi les investissements inutiles. De même, les retombées du projet au niveau stratégique sont examinées à l'aide d'outils standardisés et de données chiffrées. C'est ainsi que Telus est en train de prospérer dans l'Est du Canada. La présence d'un certain nombre d'expertises capables de traduire les besoins en une série de réponses est un avantage important permettant à Telus de soutenir ses orientations stratégiques.

L'organisation du travail au sein des équipes de projet part d'un système de valeurs qui oriente le comportement des employés et de l'ensemble de la compagnie. Les ressources externes sont appelées à adhérer aux valeurs corporatives de Telus afin d'aboutir à des résultats positifs. Cependant, il incombe aux employés de Telus de promouvoir ces valeurs et d'encourager les collaborateurs externes à les adopter. Ainsi, il serait possible de surmonter les différences et de s'adapter de la meilleure façon aux nouveaux contextes.

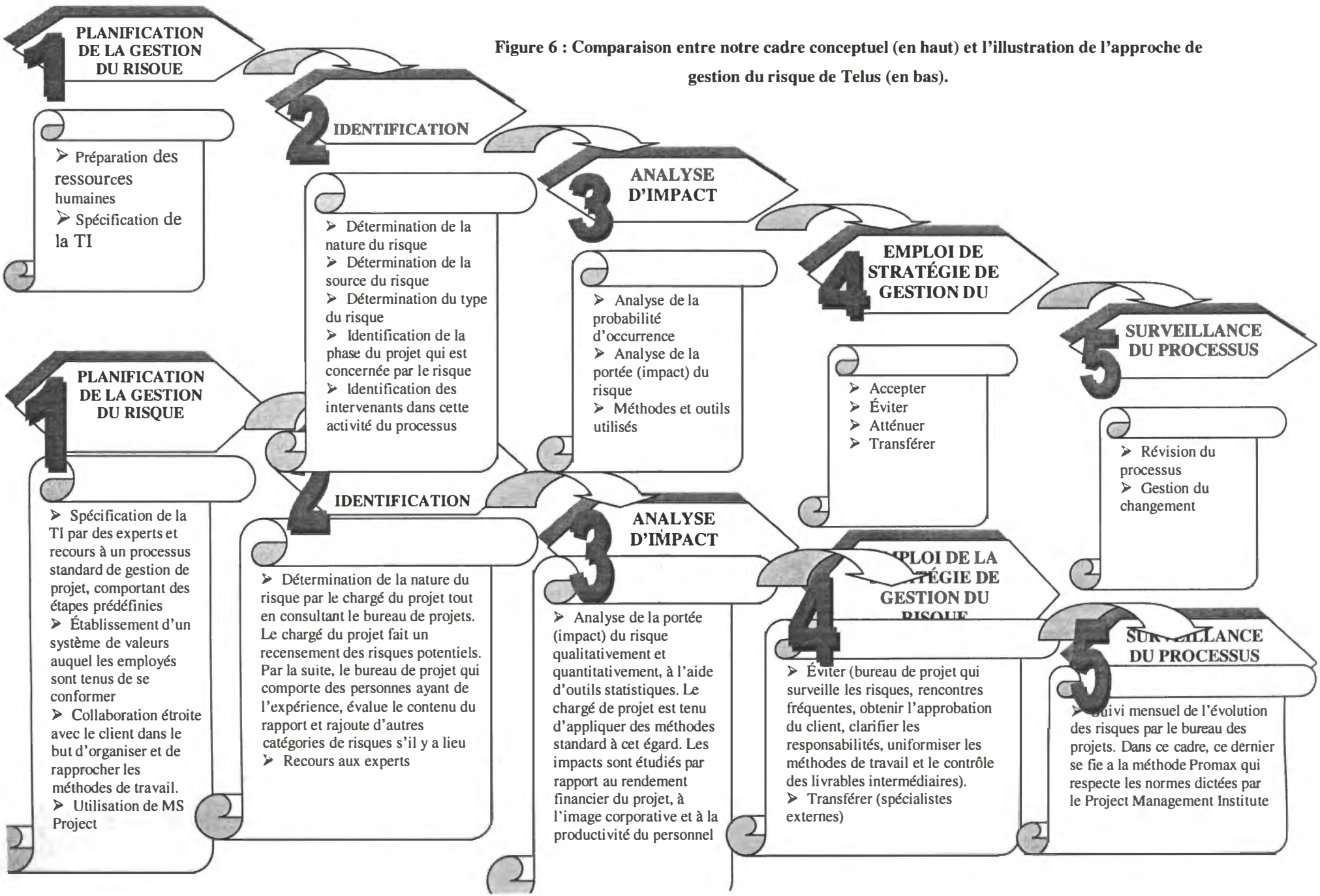
Nous pouvons constater après l'étude des facteurs clefs de succès de la gestion du risque de Telus qu'il y a beaucoup d'attention et de rigueur rattachées à ces derniers. Ils sont suffisamment maîtrisés pour soutenir l'approche de gestion du risque chez Telus. Nous nous consacrons dans ce qui suit aux différents aspects caractérisant cette approche. Celle-ci repose fortement sur la standardisation des différentes étapes du projet. En fait, ce choix est motivé par la volonté des dirigeants de la compagnie à limiter au maximum la survenance d'imprévus, en étant proactifs. D'ailleurs, les risques que nous avons pu recenser se rapportent essentiellement aux coûts et à l'échéancier. Cependant, le risque relatif à l'existence de différences culturelles est susceptible de freiner ou de bloquer carrément l'entente entre les participants au projet, ce qui peut avoir des conséquences graves si ces problèmes ne sont pas contournés dès leur émergence tout en ayant un esprit de tolérance et de coopération pour le bon déroulement du projet. Dans ce sens, Telus est soucieuse du respect des délais vu qu'elle opère à l'échelle nationale ce qui rend la perte de temps d'autant plus coûteuse qu'elle se traduit en de parts de marchés perdues et cédées à des concurrents mieux positionnées.

Par ailleurs, Telus compte aussi sur le soutien de ses experts dans l'analyse exhaustive du projet. De ce fait, nous concluons que Telus concentre essentiellement ses efforts en matière de gestion du risque au niveau des phases de planification, d'identification et d'analyse d'impact. Au niveau de la planification, l'accent est mis sur la spécification détaillée de la technologie à développer et sur l'organisation et surtout l'harmonisation des méthodes de travail au sein de l'équipe du projet. Dans ce cadre, Telus adopte un système de valeurs auquel les employés sont tenus de se conformer. Quant à l'identification, le chargé du projet travaille conjointement avec le bureau de projet dans l'identification des risques. le bureau de projet valide le recensement de risques élaboré par le chargé de projet. Dans ce sens, le bureau de projet comporte une panoplie d'expertises ayant de l'expérience et du jugement. Concernant l'étude de l'impact des risques, des méthodes standard sont appliquées par le chef de projet dans le calcul de ces derniers par rapport au rendement financier du projet, à l'image corporative et à la productivité du personnel. Cela nous permet de déduire que Telus favorise plutôt la stratégie d'évitement. En effet, à travers l'étude poussée de tous les risques qui peuvent survenir, et ce, en faisant recours aux spécialistes et à l'expérience de ses cadres, l'entreprise diminue la probabilité de réalisation de certains risques qui entravent souvent le déroulement de tout projet d'informatisation. Dans ce cadre, elle

considère que la collaboration du client est primordiale pour le succès du projet. En effet, en recensant ce que le client veut précisément et en obtenant les approbations de sa part à toutes les étapes du projet, Telus est certaines qu'elle ne sera amenée à faire des révisions au niveau du contenu de la technologie qui induisent évidemment des coûts supplémentaires.

Au niveau de la planification de la gestion du risque, l'accent est mis sur la spécification de la technologie et l'engagement du client dans le processus de production du livrable. Quant à l'identification des risques, le chargé de projet et le bureau de projets travaillent en étroite collaboration pour prévoir et discuter les risques susceptibles de freiner l'avancement du projet. Toutefois, le reste des employés qui participent à ces projets ne sont pas assez impliqués étant donné que seul le chargé de projet est tenu d'élaborer son rapport concernant l'identification des risques. Sur un autre plan, les dirigeants de Telus sont assez conscients de la nécessité du recours à la quantification et l'évaluation des impacts que peuvent avoir ces risques en cas de leur réalisation. Cela permet d'organiser les efforts et d'accorder la priorité à la gestion des risques qui sont les plus importants. Cependant, le suivi de ces risques s'établit sur une base mensuelle, et ce, tout en bénéficiant de l'avis des experts ayant déjà travaillé dans le cadre de projets similaires. Toutefois, ces derniers ne connaissent pas toujours la nature des circonstances du projet pour pouvoir formuler des idées suffisamment pertinentes quant au bon déroulement du projet. Afin de schématiser l'ensemble de ces conclusions concernant l'approche de gestion du risque de Telus, nous les retransmettons dans l'illustration graphique de notre cadre théorique dans ce qui suit.

Figure 6 : Comparaison entre notre cadre conceptuel (en haut) et l'illustration de l'approche de gestion du risque de Telus (en bas).



4.4 Commentaires généraux de la partie empirique

Le tableau suivant met la lumière sur les points saillants de la politique de gestion du risque appliquée par nos trois répondants.

Tableau 2 : Récapitulatif des trois cas décrits

Éléments de la politique de gestion du risque	UQTR	Communication Inc.	Telus Solutions d'affaires
Recours aux TI	+ site Web + Intranet	+ réseau client/serveur + différentes applications logicielles destinées à gérer les activités de communication et de marketing	+ téléphonie et réseaux informatiques basés sur Internet. + logiciels de support pour le personnel + Intranet + technologie « One source »
Maîtrise des facteurs clefs de succès	+ soutien illimité de la part de la direction - étude de rentabilité pas assez poussée basée sur une estimation sommaire des coûts. + les apports des TI sont examinés par rapport aux objectifs stratégiques de l'institution (accroissement du nombre des étudiants, avancée de la recherche, etc.) + les rencontres entre les membres des équipes de projet sont fréquentes dans le but d'éviter tout conflit. Les directeurs fonctionnels n'ont aucun pouvoir décisionnel.	-/+ réticence de la part de la direction au début. Total engagement par la suite de la part de cette dernière dans les efforts visant l'acquisition des TI. - évaluation qualitative des apports de la technologie au niveau stratégique + valorisation de la qualité des relations interprofessionnelles.	+ la direction est très soucieuse du succès de la TI à l'interne avant de l'offrir à sa clientèle. + la rentabilité de la TI est évaluée sur la base de gabarits standard pour le calcul du rendement de l'investissement. + les apports de la TI sont observés par rapport à chaque valeur corporative de Telus. + clarification poussée du mandat.
Principaux risques rencontrés	- la veille technologique - la définition du contenu de la technologie - la correspondance de la solution à la capacité de financement du client - la gestion des partenariats - le respect de la propriété intellectuelle - l'adhésion des utilisateurs.	- la sécurité du réseau de communication - la collaboration des utilisateurs	- la gestion des différences culturelles. - la gestion des changements durant la réalisation du projet.

Méthodes de gestion du risque utilisées	- absence d'une politique de gestion du risque bien définie + spécification de la TI + des séances de formation pour le personnel et les utilisateurs + coopération avec les universités québécoises + nécessité d'obtenir des approbations du client à chaque étape du projet + recours aux services des avocats dans la gestion des contrats.	+ un processus de gestion du risque entretenu quotidiennement. + préparation des ressources humaines en vue de les adapter à la TI développée. + l'observation de l'expérience d'autres entreprises ayant utilisé la même TI.	+ standardisation de toutes les étapes du projet. + le recours aux experts + la collaboration avec le client + étroite collaboration entre le chef du projet et le bureau de projet en vue d'identifier et de faire le suivi des risques sur une base mensuelle.

Les (+) représentent les points forts alors que les (-) désignent les points faibles.

En guise de conclusion de ce chapitre dédié à l'expérimentation pratique des postulats théoriques, plusieurs constatations s'imposent. Tout d'abord, il est clair à travers les trois descriptions de cas que tout projet d'informatisation est appelé à confronter une multitude de risques durant sa réalisation et le début de son exploitation. Nous avons pu remarquer dans ce cadre que ces risques dépendent du contexte dans lequel l'entreprise opère et de l'étendue de ses activités. Cependant, le risque le plus présent pour les entreprises interviewées réside dans le manque de collaboration des utilisateurs des réseaux développés ainsi que les risques techniques qui représentent une menace souvent associée à ce genre de projets. Nous notons dans ce cadre, que tous les ressources que nous avons interviewées avaient souligné le succès des projets de réseaux Internet qu'ils ont développés au sein de leurs entreprises. Ces derniers affirment qu'ils ont réussi à gérer les risques qu'ils ont rencontrés.

Les facteurs clefs de succès nécessaires à la gestion de l'ensemble de ces risques sont plus ou moins maîtrisés. Le soutien de la direction est très présent chez nos répondants. Cela est évident du fait que la majorité des entreprises de nos jours s'appuient davantage sur les TI dans leurs activités. Par conséquent, les dirigeants sont conscients qu'à l'aide de ces outils, leur compagnie sera en mesure de prospérer. C'est ce que nous avons pu constater durant les entrevues effectuées. Les répondants avaient exprimé une forte volonté de suivre la tendance technologique.

Quant aux critères de choix des TI déployés par les répondants, ils reposent plus sur la correspondance de la technologie à la mission et aux orientations stratégiques de l'entreprise. Dans ce cadre, les dirigeants essayent de faire face à la concurrence en investissant des sommes importantes dans le développement technologique. D'ailleurs, nous avions examiné dans la partie théorique la grande contribution des TI dans le repositionnement de l'entreprise par rapport aux cinq forces concurrentielles du marché identifiées par Porter (2001). Dans les cas étudiés, les réseaux de communication avaient permis d'affaiblir le pouvoir de négociation des clients dans la mesure où cela a amélioré nettement la qualité des produits offerts aux clients et de rendre ces derniers plus attentifs à cette différence.

Cependant, les études de rentabilité ne sont pas assez poussées et ne portent pas sur les aspects financiers du projet en termes de revenus futurs pouvant être engendrés. En effet, dans des projets d'une telle envergure, il existe plusieurs paramètres susceptibles d'affecter positivement ou négativement le rendement du projet. Certains de ces paramètres sont plus ou moins prévisibles tels que les taux d'intérêt, les taux d'inflation, les taux de change, etc. Par contre chez nos répondants, l'accent est mis plutôt sur des aspects qualitatifs qui, certes sont importants, mais doivent être conjugués avec des prévisions chiffrées pour qu'ils puissent être fondés.

Par ailleurs, les deux facteurs précédents ne peuvent à eux seuls produire des effets bénéfiques si l'entreprise ne dispose pas d'une structure organisationnelle favorisant la créativité. Dans les cas décrits, il y a lieu de noter la bonne définition des responsabilités qui permet d'éviter le conflit de tâches et le conflit de directives comme le prévenaient Marchewka (2003) et Buttrick (2002). C'est ainsi que les répondants affirmaient que les ressources externes étaient capables de bien s'intégrer et de fournir le rendement demandé. De plus, les conditions de travail propices sont de nature à inciter ces ressources à participer davantage aux projets futurs de l'entreprise.

Quant à l'application du processus de gestion du risque tel qu'avancé dans la partie théorique de ce travail de recherche, l'accent est plutôt mis chez nos répondants sur la planification et l'identification des risques. Les entreprises préfèrent être proactifs plutôt que réactifs face aux risques. C'est pour cette raison qu'elles ont recours durant la planification à

l'observation des apports de la technologie par rapport aux besoins de la firme, et ce, en la détaillant tel que préconisé par Feringa et al. (2001). Cela permettrait en fait selon McLaughlin (2003) d'organiser de la meilleure façon l'exploitation de la technologie mise en place. D'ailleurs, Greenstein et Vasarhelyi (2002) recommandent à la définition d'un ensemble d'instructions s'adressant aux employés afin de prévenir les risques d'ordre humain émanant des erreurs durant l'utilisation ultérieure de la TI.

Au niveau de l'identification des risques, les répondants s'appuient fortement sur les analyses des spécialistes qui s'effectuent durant tout le cycle de vie du projet tel que recommandé par Feringa et al. (2001). Cependant, la participation des utilisateurs à l'identification telle que soutenue par Fitcher (1999) et McLaughlin (2003) est plus ou moins présente. Ces derniers se fient plus aux concepteurs plutôt qu'aux utilisateurs.

Par ailleurs, sur le plan de l'étude des impacts relatifs aux risques, les efforts sont plus concentrés sur une démarche qualitative qui repose sur l'échange et l'interactivité entre les participants au projet. Quant à la stratégie de gestion du risque la plus déployée, il s'agit de la stratégie de l'atténuation qui consiste à réduire au maximum la probabilité de réalisation des risques. Dans ce cadre, nos répondants misent beaucoup sur les mesures de contrôle techniques basées sur des vérifications régulières des paramètres de sécurité des réseaux. Également, ces dirigeants ont recours à des pratiques de contrôle managériales consistant en des procédures d'utilisation prédéfinies et standardisées. Toutefois, Greenstein et Vasarhelyi (2002) rappellent que de telles mesures ne sont pas censées freiner la flexibilité dans l'utilisation de ces technologies.

Sur un autre plan, toutes les entreprises étudiées ont affirmé qu'elles préfèrent transférer parfois certains risques à une autre partie en vue de les gérer. Dans ce cadre, les moyens évoqués résident dans l'assurance et/ou la sous-traitance. Cependant, le développement par l'utilisateur final n'a pas fait partie des choix de transfert de nos répondants. Cela peut être dû à la complexité et à la sophistication des réseaux à développer, ce qui décourage les dirigeants à confier leur développement à des personnes qui ne disposent pas d'une formation appropriée.

Suite au déploiement de la stratégie de gestion du risque, il importe d'effectuer le suivi de l'ensemble du processus. Dans ce sens, nos répondants privilégient les rencontres personnalisées entre les membres de l'équipe du projet ainsi que la direction afin d'actualiser les données et de surveiller l'évolution des risques identifiés. Nous avons pu constater l'applicabilité des techniques avancées par Marchewka (2003) concernant le suivi du processus, à savoir les audits, les révisions et les rapports de situation. C'est ainsi que les entreprises étudiées assurent la continuité au niveau de leur processus de gestion du risque. Dans les entrevues effectuées, nous avons posé une question concernant leur évaluation concernant les politiques de gestion du risque qui sont déployées au sein de leurs entreprises. Dans ce cadre, nous avons noté le plein sentiment de satisfaction de nos répondants à cet effet.

En conclusion, les descriptions de cas effectuées dans le cadre de ce quatrième chapitre nous ont permis de mieux cerner les risques identifiés dans la partie théorique. Qui plus est, nous avons pu mettre la lumière sur de nouvelles catégories de risques mais qui sont spécifiques au secteur d'activité de l'entreprise. Par ailleurs, nous avons examiné la mise à profit des facteurs clefs de succès énoncés de la part de nos trois répondants. Notons que le soutien de la direction représentait le facteur ayant été le plus souligné de la part des entreprises interrogées. Enfin, nous avons étudié et commenté l'approche de gestion du risque telles que préconisée par les répondants. Dans la conclusion générale, nous récapitulons l'ensemble des arguments théoriques et empiriques relatifs à notre travail de recherche. Aussi, nous présenterons les points saillants de l'étude ainsi que les voies futures de recherche.

CONCLUSION GÉNÉRALE

Nous notons en définitive le contexte hostile qui caractérise les projets d'informatisation. En effet, plusieurs études ont été élaborées qui avaient permis d'en recenser certains risques présentés dans les premiers chapitres. Cependant, ces risques sont spécifiques dans la plupart des cas au domaine d'activité de l'entreprise ainsi qu'à la nature de l'environnement dans lequel elle opère. De plus, les risques techniques sont toujours présents pour l'ensemble des entreprises qui développent les réseaux Internet. Par ailleurs, le recours à l'étude empirique nous a permis de découvrir d'autres catégories de risques associés à ce genre de projets.

Sur un autre plan, et dans le but de bâtir une base fiable à la politique de gestion du risque, nous avons regroupé les facteurs clefs de succès sous trois rubriques, à savoir le soutien de la direction, les critères de sélection de la technologie et la gestion de la structure d'organisation du projet. Ces facteurs sont interdépendants et doivent être combinés afin d'aboutir à un résultat positif. En effet, la direction est appelée à être consciente des apports des réseaux de communication basés sur Internet et à les acquérir davantage afin d'améliorer la rentabilité de l'entreprise. Cependant, elle doit définir des critères de sélection fiables et reposant sur une évaluation exhaustive des retombées au niveau de la rentabilité et du positionnement stratégique de l'entreprise par rapport à ses clients, ses fournisseurs et ses concurrents. Dans ce sens, nous avons constaté l'importance de la procédure de choix de la technologie et sa contribution dans l'élargissement des parts de marché de nos répondants.

Par ailleurs, la réussite du projet suppose également une définition appropriée des tâches et une intégration des ressources venant de l'extérieur de l'organisation. Il revient en conséquence à la direction de bien gérer l'organisation au niveau de ses projets afin d'offrir un climat de travail propice à la collaboration mutuelle et à l'échange fructueux. La présence de ces facteurs doit être assurée par la suite durant le processus. Le processus de gestion du risque tel que défini et adapté dans ce travail de recherche comporte une succession d'étapes et intègre un ensemble d'éléments qu'il importe de maîtriser dans la mesure où il permet aux dirigeants d'optimiser la gestion des risques. Toutefois, nous avons constaté que ce processus s'adapte selon la nature des risques rencontrés ainsi qu'en fonction du domaine d'activité de la firme. Par conséquent, il serait

difficile de supposer qu'il peut y avoir un processus standard pour la gestion des risques associés aux projets d'informatisation.

Les résultats auxquels nos recherches empiriques ont abouti, montrent que les dirigeants sont de plus en plus conscients de l'importance du recours à une étude exhaustive des risques. En effet, nous avons pu constater que ces risques sont nombreux dans le cas des projets visant le développement de la technologie Internet au sein des entreprises. Les dirigeants mettent beaucoup l'accent sur la nécessité de l'efficacité de la technologie sur le plan stratégique ainsi que sur la bonne définition du mandat et des responsabilités. Toutefois, les approches utilisées par les entreprises en vue de les contourner diffèrent selon la nature des risques rencontrés. De plus, le transfert de ces risques à une autre partie représente un recours privilégié de la part de ces dernières.

Cependant, notre travail de recherche comporte certaines limites qu'il importe de les déterminer. Dans ce cadre, nous notons que notre recherche empirique ne s'est pas basée sur des données chiffrées du risque. En effet, l'accès relativement difficile à ce genre de données ainsi que l'absence d'études quantitatives faites sur les risques auprès des entreprises étudiées, ont rendu difficile un tel recours. De plus, la notion du risque ne peut pas être mise en relation avec des facteurs explicatifs. D'ailleurs, les auteurs que nous avons consultés n'ont pas tenté de modéliser la dynamique des risques en raison de sa forte dépendance du contexte spécifique du projet. Également, notre étude n'a porté que sur trois cas d'entreprises. Cela rend difficile la généralisation de nos résultats. En effet, les résultats auxquels nous avons abouti concernant les risques et les modes de leur gestion, sont très dépendants de la nature d'activité de l'entreprise questionnée et de sa situation interne. Toutefois, des contraintes de temps et le manque de contacts ont limité le nombre des entreprises ayant répondu à notre question de recherche. De plus, nous n'avons interrogé qu'une seule ressource dans chaque entreprise étudiée. Par exemple, nous n'avons pas questionné les utilisateurs de la technologie implantée sur les risques qu'ils rencontrent le plus souvent. Toutefois, il est évident que les personnes interviewées ont une connaissance suffisante des projets d'informatisation entrepris au sein de leurs entreprises.

Les retombées relatives à ce travail sur la recherche en matière de gestion du risque se situent à plusieurs niveaux. Premièrement, nous avons avancé par présence de trois facteurs clefs de succès à la gestion du risque dans le cadre des projets d'informatisation en entreprise, à savoir, le soutien de la direction, le choix de la technologie et la gestion de la structure d'organisation du projet. Ces facteurs représentent des préalables importants dans la gestion du risque. Dans ce cadre, nous avons déduit à partir des arguments de plusieurs auteurs que certains éléments soutiennent la politique de gestion du risque au sein de l'entreprise. Ces éléments relèvent de la situation interne de l'organisation. Notre contribution consiste essentiellement dans la classification de ces éléments en trois facteurs clefs de succès. Deuxièmement notre modèle de recherche adapté de Marchewka (2003) a regroupé tous les éléments de gestion du risque avancés par d'autres auteurs. En effet, nous avons réuni et organisé les apports de tous les auteurs que nous avons consultés dans notre modèle de recherche pour former un cadre théorique de gestion du risque qui soit appliqué à tous les projets d'informatisation. Troisièmement, nous avons approfondi l'identification des risques inhérents à la technologie Internet. Dans ce cadre, nous avons classifié ces risques selon leur nature qu'ils soient financiers, techniques, de coût et d'échéancier. Néanmoins, cet effort était soutenu par les témoignages recueillis auprès des répondants à nos entrevues. En effet, cela nous a permis de constater la présence d'autres formes de risques dans le cadre de la technologie Internet.

En ce qui concerne de futures pistes de recherche, certains risques restent à étudier. D'ailleurs, c'est ce que nous avons constaté au terme de cette étude. En effet, nous citons dans ce cadre l'exemple des risques relatifs aux différences culturelles qui méritent d'être approfondies davantage, et ce, pour deux raisons. Premièrement, les conséquences de tels risques sont graves et leur portée est imprévisible. Tout manque ou absence d'entente au sein de l'équipe du projet est susceptible de bloquer tout l'investissement technologique. Comme nous l'avons vu dans le cas de Telus Solutions d'affaires, certaines méthodes de travail sont parfois difficiles à faire accepter auprès des collaborateurs étrangers. La deuxième raison consiste dans la prolifération que connaissent les projets à vocation internationale actuellement. D'ailleurs, nous notons la multiplication des ententes internationales et l'intensification des accords de libre échange entre les pays et en particulier les pays développés. Cela serait propice à la réalisation de projets à l'échelle mondiale faisant intervenir des individus ayant des profils culturels différents. Un tel

constat suppose la possibilité de l'existence de certains conflits d'ordre culturel qui peuvent se créer entre ces individus. Il importe alors d'y penser et d'en fournir les explications ainsi que les solutions appropriées. C'est dans ce cadre que s'inscrit la recherche effectuée par Hofstede (1994)[29] qui avait tenté de définir quatre aspects culturels à partir desquels il est possible de repérer les différences culturelles entre les individus. Cette étude pourrait constituer une base de départ pour tout effort futur consistant à prospecter la question relative à la gestion des différences culturelles au sein des équipes de projet d'informatisation.

[29] Hofstede, G. 1994. Vivre dans un monde multiculturel. Les éditions de l'organisation, Paris.

RÉFÉRENCES

Aboubekr M. et Rivard S. 2002. Commerce Électronique et Conflits de Canaux de Distribution. Publications Cirano, Montréal, no 2002RP-09 :
http://www.cirano.qc.ca/pdf/publication/2002RP-09.pdf (Consulté en Juin 2003)

Aboubekr M. et Rivard S. 2003. Pertinence de l'utilisation d'Internet comme canal de distribution : cas du secteur des assurances. Publications Cirano, Montréal :
http://www.cirano.qc.ca/pdf/publication/2003s-37.pdf (Consulté le 16 Novembre 2003)

Alavi, M. (1985). Some thoughts on quality issues of end-user developed systems. *Présenté dans le cadre de la Conférence annuelle Computer Personnel.* Minneapolis, Minnesota.

Association pour la recherche sur l'emploi des techniques. 1986. *Réussir l'informatisation de la PME.* Paris : Les éditions d'organisation.

Aubert B. et Dussart A. 2002. Systèmes d'information Inter-Organisationnels. Publications Cirano, Montréal : http://www.cirano.qc.ca/pdf/publication/2002RB-01.pdf (Consulté en Juin 2003).

Bacca, E., (2001). A check list of must have features for your Intranet. www.intranetjournal.com (Consulté le 29 Septembre 2003).

Barki, H., Bourdeau S. et Rivard S. (2003). Évaluation du risque en gestion de projet. Publications Cirano, Montréal, no 2003s-47 :
http://www.cirano.qc.ca/pdf/publication/2003s-47.pdf (Consulté le 26 Novembre 2004)

Barki, H. et Hartwick, J. (1990). Developing measures of user participation and user involvement. *Cahier GReSI,* HEC Montréal, no 90-11.

Barki, H., Rivard, S. et Talbot, J. (1992). Risque, mode de gestion et succès d'un projet d'informatisation. *Cahier GReSI,* HEC Montréal, no 92-07.

Barki, H., Rivard, S. et Talbot, J. (1993). Toward an assessment of software development risk. *Journal of Management Information Systems*, vol.10, no 2, pp.203-225.

Barnes, H., (2001). Employing strategic content management for successful Intranets. Tiré du site: http://www.intranetjournal.com/
Date de consultation : 29/09/2003

Benaroya F. et Landau J., 1999. *L'échange international.* Presses universitaires de France : Paris. France.

Boehm, B. W. 1989. *A spiral model of software management and enhancement.* IEEE Computer Society Press : Washington, DC.

Buttrick R. 2002. *Gestion de projet en action.* Éditions Village Mondial : Paris, France.

Campbell, D. (1988). A task complexity: A review and analysis. *Academy and Management Review,* vol.13, pp 40-52.

Chang S. et Gable G. 2001. A comparative analysis of major ERP lifecycle implementation, management and support issues in Queensland government. Pacific Asia conference on information systems.

Chevalier, M. (2001). L'impartition, Quoi, Comment et Pourquoi? *Conférence présentée dans le cadre du congrès annuel de l'AIPVQ.* Montréal (Québec), Canada : Complétif.

Chokron, M. (1996). Planification stratégique des systèmes d'information. Une méthode hiérarchisée de planification des systèmes d'information. *Cahier GReSI,* n°96-03.

Choo, G. 2001. It's A Risky Business. www.systemcorp.com/frame-site/downloads/choo_p.html

Clemons E. K. 1995. Using scenario analysis to manage the strategic risks of reengineering. *Sloan management review. 36; 4, 61-71.*

Cosgrove W. 2001. ERP Progress. *CIO magazine report.*
http://www2.cio.com/research/surveyreport.cfm?id=31

Damsgaard, J. et Scheepers, R. (1999). A Stage Model of Intranet Technology Implementation and Management. *7ème édition de la conférence européenne sur les systèmes d'information.* Copenhagen Business School, Copenhagen, Denmark.

Darracott, G., (2003). Opinion: It pays to make your Intranet attractive. *New Media Age.* Date de consultation : 10/10/2003.

Davis, G. B. (1982). Caution: User-developed decision support systems can be hazardous to your organization. *Présenté dans le cadre de la 17ème conférence annuelle sur la science des systèmes.* Honolulu, Hawaii.

Davis, G. B. et Olson, M. (1985). *Management information systems: Conceptual foundations, structure and development.* New York: Mc Graw-Hill Press.

Desq S. (1992). Le succès de l'informatique utilisateur. *Cahier GreSI,* HEC Montréal, no 92-05.

Deming W. 1996. Du nouveau en économie. *Économica* : Paris. France.

Doherty, N. A. (1985). *Corporate risk management, a financial exposition.* New York : Mc Graw-Hill book company.

Duane A. et Finnegan, P (2000). Managing intranet technology in an organizational context. *Tiré du site*: www.mis.coventry.ac.uk
Date de consultation : Juin 2003

Fatout, M. F. (1995). Using Limits and Structures for Empowerment of Children in Groups. *Social Work with Groups.* Vol.17, no 4, pp. 55-69.

Fitcher, M. (2003). The whys and hows of Intranet marketing. *Online Journal.* Date de consultation : 10/10/2003.

Feringa, A., Goguen, A., et Stonebumer, G. (2001). Risk management guide for information technology systems. *US Government Printing Office*: Washington, USA.

Franklin, C., Jr. 1997. Emerging Technology : Enter the Extranet. *CIO Magazine*, http://www.cio.com/ (Consulté le 16 Novembre 2003).

Gauthier, B. 2002. *Recherche sociale : de la problématique à la collecte de données, 3ème édition.* Presses de l'Université du Québec : Québec, Canada.

Godes D., Ofek E. et Sarvary M. 2003. Products vs. Advertising: Media Competition and the Relative Source of Firm Profits. Social Science Research Network Electronic Paper Collection: http://ssrn.com/abstract=386561 (Consulté le 16 Novembre 2003).

Gorden, R., L. 1980. Interviewing *: Strategy, Techniques and Tactics.* Homewood Dorsey press: USA.

Greenstein M. et Vasarhelyi M. 2002. *Electronic Commerce, security, risk management and control* (2ème edition). McGraw-Hill : NY.

Helper, S. (1991). Strategy and irreversibility in supplier relations : the case of the US automobile industry. *Business History Review*, vol.65, n°4, p.781-824.

Henry, A. (1999). Intranet management made easier. *Tiré du site:* www.itmanagement.earthweb.com
Date de consultation : 29/09/2003

Hofstede, G. 1994. Vivre dans un monde multiculturel. Les éditions de l'organisation, Paris.

Hyot R. et Khang H. (1999). On the Demand for Corporate Property Insurance. *Journal of Insurance Regulation* 16: 145-189.

Jones, T. C. 1994. *Assessment and Control of Software Risks.* Upper Saddle River, N.J: Yourdon Press/Prentice Hall.

Karolak W. 1996. *Software engineering risk management.* Computer Society Press : California, USA.

Kasper, G. M. (1985). The effect of user-developed DSS applications on forecasting decision-making performance in an experimental setting. *Journal of Management Information Systems*, vol. 2, No. 2, pp. 26-39.

Keen, P. (1983). A policy statement for managing microcomputers. *Computer-world*, vol. 17, No. 20, pp. 35-39.

Keil M., Mann J. et Ray A. 2000. Why software projects escalate. *MIS Quaterly,* vol.24, no 4, pp.631-664.

Lanza, R. B. 2001. Reviewing a Project Risk Management System. www.Auditsoftware.net/infoarchive/articles/projmgmt/files/riskmgmt.htm (Consulté en 2003)

Laudon K. et Laudon J. 2000. *Les systèmes d'information de gestion. ERPI* : Québec, Canada. Adaptation française par Lin Gingras.

Lebrun, J., Rivard, S. et Talbot, J. (1990). Measuring the quality of user-developed applications. *Cahier GreSI*, HEC Montréal, n 90-12

Leibenstein, H. (1966). Allocative efficiency vs X-efficiency. *AER*, vol.56, n°3, P.392-415.

Levine, S. 1975. Financial analyst's handbook. *Homewood* : USA.

Maiwald, E. 2001. Sécurité des réseaux. *Campus Press* : France,.

Mantel S. et Meredith J. 2000. *Project management : a managerial approach* (4ème édition). John Wiley & Sons : NY

Marchewka, J. 2003. *IT project management, providing measurable organizational value*. John Wiley & Sons : NY

Martin, M. 1998. Entreprise resource planning. *Fortune*, vol.137, no 2, pp.149-151.

McLaughlin, M. (2003). Apply usability methodologies in Intranet information architecture in a real world context, Partie I. *Tiré du site*: www.intranetjournal.com
Date de consultation : 29/09/2003

Moreau, É. (2000). Les liens entre l'utilisation des systèmes d'aide à la décision intelligents et le travail intellectuel. *Thèse de doctorat, Montréal, UQAM.*

Nelson M. (1999). Extrapolating the Future of Extranets. *Info World Electric*, http://cgi.infoworld.com/ (Consulté le 16 Novembre 2003)

Nelson, R., et Todd, P. (1999). Strategies for managing EUC on the Web. *Journal of End User Computing*. Vol.11, no 1, pp.24-31.

O'Brien, J. 1995. *Les Systèmes d'information de gestion, la perspective du gestionnaire-utilisateur.* Québec : Éditions du renouveau pédagogique.

Paquin, M. 1990. *Gestion des technologies de l'information.* Ottawa : Les éditions Agence d'Arc.

Poitevin, M. (1999). *Impartition: Fondements et analyses.* Sainte-Foy : Presses de l'Université Laval.

Porter, M. 1980. *Competitive strategy.* NY: The Free Press.

Pradels, J. L. 1981. *L'informatisation des entreprises : qualité, productivité, rentabilité des projets.* Paris : Éditions EYROLLES.

Project Management Institute. 2000. Project Management Body of Knowledge. http://pmi.org/prod/groups/public/documents/info/PP_CompletedProjectsPMBOK2000.asp

Rondeau A. 2001. Transformez votre organisation grâce aux TI. Guides IQ : Québec, Canada.

Ryan, B. 1997. *The Corporate Intranet.* John Wiley and Sons : NY.

Schirripa, F. et Tecotzky, N. (2000). An Optimal Frontier. *The Journal of Portfolio Management.* Vol.26, no 4, pp.29-40.

Simons, R. (1995). Levers of control. *Harvard Business School Press.*

Waltner, C. (1999). Control the flow. *Consulté à partir de la base de données ABI/Inform : Information week.* Date de consultation : 10/10/2003.

Ward, T. (2003). Five winning Intranet characteristics. *Tiré du site*: www.intranetjournal.com *Date de consultation* : 29/09/2003

Wideman, R. M. 1992. *Project and Program Risk Management: A Guide to Managing Project Risks and Opportunities.* Newtown Square, Pa.: Project Management institute.

Zrimsek, B., Phelan, P., Karamouzis, F. et Frey, N. 2001. Estimating the time and the cost of ERP and ERP II projects: A 10-step process. Publications du Gartner Group.

Verisign, Inc. (1999). Guide to securing Intranet and Extranet Servers. *Tiré à partir du site*: www.pttrust.com/Guides/Guide4.pdf

ANNEXES

ANNEXE A
GUIDE DES ENTREVUES

1. Quelle place occupe les technologies d'information au sein de votre organisation?

2. Situez les apports des réseaux de communication basés sur Internet pour votre organisation?

3. Dans quelle mesure ces réseaux sont-ils soutenus par la direction? Illustrez

4. À partir de quels critères avez-vous opté pour cette technologie?

5. Dans ce cadre, avez-vous procédé à une étude de rentabilité au départ?

6. Également, avez-vous examiné les apports potentiels de ces réseaux sur le plan stratégique pour votre organisation?

7. De quelle façon gérez-vous la structure organisationnelle dans le sens où le projet fait appel à des ressources de l'extérieur, ce qui serait susceptible de créer certains conflits?

8. Citez les principaux risques auxquels vous avez fait face durant l'implantation des réseaux de communication dans votre entreprise ?

9. Entretenez-vous une politique ou un processus destiné à la gestion de l'ensemble de ces risques au sein de votre entreprise?

10. Si oui, quels sont vos motifs?

11. Comment planifiez-vous la gestion du risque? et quels sont les éléments sur lesquels vous misez le plus pour réussir la gestion du risque?

12. De quelle façon identifiez vous les risques auxquels fait face votre projet? Faisiez vous des distinctions dans le but de bien catégoriser ces risques ?

13. Quelles sont les personnes qui interviennent lors de l'identification des risques?

14. De quelle façon analysez-vous les impacts relatifs à ces risques? Aviez-vous recours à certaines méthodes de calcul spécifiques dans ce cadre? Citez des exemples

15. Citez parmi ces stratégies de gestion du risque celles que vous privilégiez et donnez des justifications :

    a) Accepter ou ignorer
    b) Éviter
    c) Atténuer
    d) Transférer

16. De quelle façon surveillez vous tout le processus de gestion du risque? quelles sont vos techniques dans ce cadre?

ANNEXE B

GRILLE D'ÉVALUATION DES REPONSES

Numéro de la question	Critères d'évaluation et d'interprétation des réponses	Auteurs afférents
1	Rédiger l'introduction et constater l'importance qu'accordent les dirigeants pour les TI.	Aubert et Dussart (2002) ; Marchewka (2003), Aboubekr et Rivard (2002) et Laudon et Laudon (2001) et Bacca (2001)
2	Comprendre l'effet de l'introduction des TI sur la performance de l'organisation et sur le niveau de collaboration et de communication entre les employés.	Aubert et Dussart (2002) ; Marchewka (2003), Aboubekr et Rivard (2002) et Laudon et Laudon (2001) et Bacca (2001)
3	1. assimiler la façon par laquelle les facteurs clefs de succès de la gestion du risque sont maîtrisés par les dirigeants. 2. recenser et analyser les moyens agencés par la direction en vue d'assurer du soutien au projet d'informatisation. 3. voir si la direction est suffisamment tolérante vis à vis de l'équipe de projet en ce qui attrait aux délais d'exécution et aux erreurs. 4. avoir une idée sur la qualité du climat de travail ainsi que les échanges entre les différents intervenants au projet (équipe de projet, direction, utilisateurs, etc.), ce qui représente un gage pour la rentabilité de la technologie implantée.	Jones (1994) ; Lanza (2001) ; Choo (2001) et Buttrick (2002)
4	Comprendre les critères de sélection des TI adoptées par l'entreprise.	Mantel et Meredith (2000) ; Pradels (1981) ; ARTE (1986) ; Paquin (1990) ; Chokron (1996) ; O'Brien (1995) ; Porter (1980) et Laudon et Laudon (2000)
5	1. analyser le niveau et la qualité de la planification de la part des dirigeants (existence ou non d'une étude de rentabilité au départ). 2. étudier les techniques de calcul des coûts (méthodes d'agrégation, rubriques considérées, logiciels utilisés, etc.) 3. recenser et analyser les indicateurs financiers utilisés par la firme et les étudier. 4. demander des informations concernant l'exactitude des	Mantel et Meredith (2000) ; Pradels (1981) et ARTE (1986)

	estimations faites dans le cadre des projets d'informatisation déjà entrepris.	
6	1. commenter le niveau de conscience des dirigeants quant à la mission et les orientations stratégiques de la firme lors du choix de la TI à implanter. 2. comprendre les critères de sélection de l'organisation par rapport à l'ajustement de la technologie à la stratégie de marché mise en place, et les comparer dans un deuxième temps aux critères proposés dans la théorie. 3. demander si certaines technologies ont permis au passé à l'entreprise de générer un avantage concurrentiel sur le marché. 4. conclure en jugeant la qualité de l'ajustement de la technologie à la stratégie de la firme.	Paquin (1990) ; Chokron (1996) ; O'Brien (1995) ; Porter (1980) et Laudon et Laudon (2000)
7	1. décrire le niveau de conscience des dirigeants des conflits pouvant être crées par l'existence d'une structure matricielle dans l'organisation. 2. savoir si l'organisation développe une culture d'entreprise favorisant l'intégration de ressources externes durant les projets d'informatisation. Commenter et évaluer les constatations. 3. analyser les politiques mises en œuvre dans ce contexte ainsi que la qualité de la gestion des conflits, et ce, en vue d'assurer un niveau de communication interpersonnelle motivant pour l'ensemble des intervenants. 4. conclure en analysant la qualité de la planification organisationnelle dans l'entreprise.	Buttrick (2002) et Marchewka (2003)
8	1. recenser les risques et les catégoriser (risque financier, risque technique, risque de coût et risque d'échéanciers). 2. comparer ces risques à ceux avancés dans la partie théorique afin de pouvoir commenter la capacité des dirigeants à connaître la nature des risques auxquels ils font face. 3. spécifier et juger la qualité des réseaux mis en place.	Laudon et Laudon (2000) ; Karolak (1996) ; Chang et Gable (2001) ; Nelson (1999) ; Franklin (1997) ; Greenstein et Vasarhelyi (2002) et Martin (1998)

9	1. savoir si l'organisation est consciente de l'importance de la définition d'une politique de gestion du risque qui soit efficace en vue de gérer les événements indésirables. 2. comprendre si cette politique est axée sur la pro activité ou plutôt sur la réactivité, commenter et évaluer. 3. interpréter l'importance qu'accordent les dirigeants à la gestion du risque.	Buttrick (2002) ; Jones (1994) ; Greenstein et Vasarhelyi (2002) ; Marchewka (2003) ; Choo (2001) et Lanza (2001)
10	Comparer les arguments avancés par les répondants à la théorie et juger leur cohérence et leur opportunité.	Buttrick (2002) ; Jones (1994) ; Greenstein et Vasarhelyi (2002) ; Marchewka (2003) ; Choo (2001) et Lanza (2001)
11	1. voir et analyser la façon par laquelle la direction sensibilise l'ensemble des intervenants de l'importance de la gestion du risque. 2. connaître la place qu'occupe le facteur humain le processus de gestion du risque étant donné qu'il représente le facteur le plus difficile à gérer. 3. analyser les modes de gestion des ressources humaines, prévus dans le l'objectif de réussir le processus de gestion du risque. 4. savoir si l'entreprise procède ou pas à la spécification détaillée de sa technologie à implanter dans le but de bien cerner les différents attributs de la technologie. Rappelons qu'une bonne compréhension des spécificités de la technologie soutient le processus de gestion du risque et permet de bien préparer et de bien fonder l'étape suivante à savoir l'identification des risques.	Greenstein et Vasarhelyi (2002) ; Barnes (2001) et Feringa et al. (2001)
12	1. étudier la façon par laquelle l'organisation identifie les risques inhérents à la TI à implanter en ayant une idée sur ses méthodes et ses techniques dans ce cadre. 2. comparer par la suite ces méthodes et techniques à ceux avancés dans la théorie et rédiger des recommandations. 3. voir si l'organisation procède à certaines distinctions ayant attrait à la source, à la nature ou au type des risques, ou bien par rapport au cycle de vie respectif durant lequel interviennent les risques. Nous rappelons qu'une telle distinction serait de nature à optimiser l'activité d'identification des risques.	Buttrick (2002) ; Jones (1994) ; Greenstein et Vasarhelyi (2002) ; Marchewka (2003) ; Feringa et Al. (2001) et Ward (2003)

13	Savoir si l'équipe de projet ainsi que les utilisateurs potentiels de la TI à implanter sont suffisamment consultés dans l'identification des risques.	Barnes (2001) ; Fitcher (1999) et McLaughlin (2003)
14	Recenser et juger l'opportunité du choix des méthodes d'analyse de l'impact des risques identifiés par l'organisation. L'interprétation de ces méthodes s'effectuera en ayant regard sur la nature des risques cités préalablement par les répondants.	Buttrick (2002) et Feringa et al. (2001)
15	1. En comparant les réponses à la théorie relative à la stratégie adoptée, nous commenterons le degré d'application de la stratégie telle que énoncée par les auteurs respectifs. 2. Nous évaluerons également la pertinence de cette stratégie par rapport à l'objectif poursuivi à savoir la réduction des risques.	Marchewka (2003) ; Buttrick (2002) ; Feringa et Al. (2001) ; Laudon et Laudon (2000) ; Hoyt et Khang (1999) ; Poitevin (1999) et Lebrun, Rivard et Talbot (1990)
16	1. juger l'importance qu'accorde les dirigeants à la surveillance et au contrôle du processus de gestion du risque. 2. analyser les techniques mises en place dans ce cadre. 3. commenter la gestion du changement dans l'organisation et décrire son niveau de flexibilité.	Greenstein et Vasarhelyi (2002) ; Marchewka (2003) et Feringa et al. (2001)