



Savoir gérer le risque pour éviter les écueils des TI

En 2002, la division néerlandaise de la filiale Quest de la multinationale ICI implante une solution de gestion de type ERP de SAP pour supporter les processus de sa chaîne logistique. Quest était alors un client de SAP depuis 1972. Au cours des neuf mois qui ont suivi l'entrée en service de la solution, l'entreprise vit des problèmes majeurs quant à l'expédition, la manutention, et le stockage de ses produits à un point tel que l'entreprise a perdu des clients majeurs au début de 2003. Une grande partie de la solution ERP fut ensuite abandonnée. Les pertes encourues? 45 millions de livres sterling, une perte de 39 % de la valeur boursière de l'entreprise, la démission des chefs de la direction de Quest et de la compagnie mère ICI, et la vente de la filiale Quest à un compétiteur.

En 2005, suite à l'acquisition de la compagnie K-Mart, la compagnie Sears, Roebuck and Co. annule un contrat d'impartition d'une durée de 10 ans et d'une valeur de 1.6 milliard de dollars américains auprès du fournisseur de services Computer Sciences Corp. (CSC), seulement 11 mois après l'avoir signé. Les pertes encourues? 96 millions de dollars américains en frais d'annulation, une relation tendue avec un fournisseur de service, et une dispute légale toujours en cours alors que CSC tente d'obtenir un dédommagement de 80 millions de dollars américains.

Plus tôt cette année, TJX, la compagnie mère des chaînes de magasins Winners et HomeSense, a annoncé avoir été victime d'une faille de sécurité dans ses systèmes. Au moins 45,7 millions de numéros de cartes de crédit et de débit, ainsi que des renseignements personnels, des clients de TJX ont été volés par des pirates informatiques pendant plusieurs années. Les pertes encourues? À ce jour, près de 256 millions de dollars américains, mais certains analystes de Gartner et Forrester prévoient des pertes de 1 milliard de dollars américains.

Bref, il peut être très coûteux de ne pas faire attention aux risques liés aux TI. De plus, ces histoires d'horreur ne sont que la pointe de l'iceberg, la plupart des échecs et des problèmes liés aux TI n'étant pas recensés dans les médias. Que ce soit pour éviter l'échec d'un projet d'implantation de progiciel, la signature d'un contrat d'impartition contraignant, ou

Pour limiter les résultats indésirables dans le cadre d'un projet de TI, il importe d'appliquer une méthodologie efficace de gestion du risque et de développer une culture vigilante qui vise l'identification et la résolution de problèmes. Mise en contexte.

des failles de sécurité informatique, la gestion du risque est maintenant devenue une nécessité.

Une gestion du risque adéquate requiert deux éléments. Premièrement, il faut se doter d'une méthodologie rigoureuse et systématique, qui permet d'identifier la nature du risque encouru, d'évaluer son importance, et de stimuler la prise de décision quant aux opportunités d'atténuation. Deuxièmement, l'entreprise doit miser sur une culture vigilante, où la communication est fréquente et honnête, où les contributions de chacun sont respectées, et où l'expertise a plus de valeur que l'autorité.

Une méthodologie rigoureuse

La gestion du risque lié aux TI nécessite une approche différente de celle qui peut être adoptée pour gérer le risque financier d'une entreprise. Puisque les données historiques et les balises permettant les comparaisons sont rares, une méthodologie particulière est requise pour évaluer le risque, telle que celle développée par mes collègues Benoit Aubert, Suzanne Rivard, et Michel Patry de HEC Montréal.

Une méthodologie de gestion du risque commence généralement par l'identification des résultats que le projet cherche à accomplir ou à éviter. Par exemple, pour l'implantation d'un progiciel de gestion intégrée comme SAP ou Oracle, il y a le respect de l'échéancier ou du budget. Une fois que les résultats du projet sont énumérés, il faut attribuer à chacun de ces résultats, une cote représentant l'impact que pourrait avoir la réalisation de ce résultat indésirable.

Deuxièmement, il faut identifier les facteurs qui peuvent influencer la probabilité que ces résultats ne se concrétisent pas. En d'autres mots, il faut définir les caractéristiques de ces projets, comme la complexité des processus et l'expertise de l'équipe de projet. Ces facteurs proviennent généralement soit de la nature du projet ou du contexte dans lequel le projet est mené. Certains facteurs de risque sont plus influents envers un résultat plutôt qu'un autre, c'est pourquoi il est important

SUITE À LA PAGE 32



Jean-Grégoire Bernard
(jean-gregoire.bernard@hec.ca)

Professeur adjoint à HEC Montréal et chercheur au CIRANO, le Centre interuniversitaire de recherche, de liaison et de transfert des savoirs en analyse des organisations.

Ne manquez pas tous les volets de cette série spéciale d'articles sur la gestion stratégique des TI au sein des organisations. Pour des informations complémentaires, visitez également notre site Web au www.directioninformatique.com.

DIRECTION INFORMATIQUE

En collaboration avec

HEC MONTRÉAL

Présentée par



SÉRIE gestion stratégique des TI EN UN COUP D'ŒIL

Septembre 2007 1 • **Introduction** - Alignement des TI et des besoins d'affaires.

2 • **Gestion du changement** - Une vision concrète et cohérente du changement.

Octobre 2007 3 • **Gestion de projet** - Comprendre l'art et la science de la gestion de projets et les processus de projet.

4 • **Gestion du risque** - Identification et compréhension des principaux éléments de risque reliés aux technologies.

Novembre 2007 5 • **Gestion de relations avec les partenaires** - Survol du processus de sélection de partenaire.

6 • **Entrepreneurship et Innovation** - Comment utiliser une culture d'entrepreneuriat pour stimuler l'innovation.

Déc.-Janv. 2007 7 • **Tendances et globalisation des marchés** - Le marché mondial en constante évolution et le positionnement du Québec.

8 • **Bilan et conclusion** - Préoccupations éthiques et questions de gouvernance et d'intégrité.

Savoir gérer le risque pour éviter les écueils des TI

SUITE DE LA PAGE 31

d'identifier les liens qui existent entre les facteurs et les résultats indésirables.

Troisièmement, il faut attribuer une cote à chaque facteur de risque qui reflète la présence ou l'absence de ce facteur pour le projet. Cette cote se substitue à l'usage des probabilités, que la recherche en psychologie cognitive démontre que nous avons de la difficulté à interpréter intuitivement.

Cette procédure permet d'obtenir une carte d'exposition au risque à partir de laquelle il est possible d'effectuer des arbitrages entre les différents résultats indésirables du projet. C'est à ce moment qu'il est possible d'évaluer l'efficacité de différentes pratiques de gestion pour réduire le risque.

Certaines pratiques de gestion permettent d'atténuer la probabilité qu'un résultat indésirable se réalise. Par exemple, augmenter le budget de formation des utilisateurs permet de réduire la probabilité de résistance à l'utilisation du progiciel.

D'autres pratiques permettent d'atténuer l'impact d'un résultat indésirable sur la viabilité de l'entreprise. Par exemple, la prise d'une assurance en cas de sinistre ou la mise en place de plans de contingences permettent de réduire l'impact de la concrétisation d'un sinistre, mais n'affectent en rien la probabilité d'un sinistre.

Cette méthodologie peut être accomplie par quelques experts, ou encore par le biais d'un comité de représentants des unités d'affaires impliquées dans le projet ou le système à l'étude. Il est important cependant d'effectuer un suivi et de mettre à jour régulièrement l'évaluation du risque. Utilisée activement, la méthodologie devient un véritable tableau de bord qui permet de rechercher les problèmes inattendus et de prévenir leur escalade.

Plusieurs études menées par les chercheurs de HEC Montréal et du CIRANO ont permis d'identifier les facteurs de risque liés à l'impartition de services informatiques (a), à l'implantation de progiciels de gestion intégrée (b), et aux risques d'affaires (c).

Une culture vigilante

Une entreprise ayant une culture propice à la gestion des risques aura tendance à valoriser les trois pratiques suivantes.

1 La communication est fréquente, honnête, opportune, et axée sur la résolution de problèmes. Pour s'assurer de conserver un portrait global et complet du risque, il est important de faciliter une communication ponctuelle entre chacun des acteurs impliqués dans le projet à l'étude.

Il est malheureusement très facile de sous-estimer les besoins en communication, car il est nécessaire de prendre la perspective des autres pour pouvoir comprendre ce que nous tentons de leur communiquer. Or, la recherche en psychologie sociale démontre que nous avons beaucoup de difficulté à prendre la

perspective des autres, puisque nous avons tendance à projeter nos connaissances chez autrui. Dans un contexte d'affaires où le temps est compté, où les relations interpersonnelles peuvent être tendues, où les expertises sont hétérogènes, cette difficulté est accentuée.

2 Le respect des contributions de chacun est valorisé. Il est important que le contexte dans lequel se déroule la gestion du risque n'en soit pas un où « on tire sur le messenger ». En d'autres mots, il est important que les personnes qui participent à l'exercice de gestion du risque puissent parler sans peur d'être blâmées et en toute confiance; c'est-à-dire qu'ils aient un sentiment de sécurité. La recherche de critiques, des problèmes, et des erreurs est encouragée.

De plus, la notion de respect ne se limite pas à fournir un forum où les opinions dissidentes sont émises sans rétribution; cela signifie aussi être prêt à faire confiance et à considérer ces informations comme légitimes. Si on tire sur les messagers et on entend sans écouter, le silence s'installera et seules les nouvelles qui permettent de faire bonne impression feront surface.

3 L'expertise a plus de valeur que l'autorité. Pour que la gestion du risque soit une réussite, il est aussi important que les solutions aux problèmes soient sollicitées auprès de ceux qui ont le plus d'expertise pour les résoudre et non auprès de ceux qui ont le plus d'autorité dans la hiérarchie du projet ou de l'entreprise. Cela signifie que l'opinion d'un technicien ou d'un analyste à propos d'une vulnérabilité ou d'un facteur de risque peut avoir préséance sur celle d'un directeur. Cette approche n'est pas facile à réaliser en pratique, mais les entreprises qui maîtrisent la gestion du risque la chérissent.

L'adoption active d'une méthodologie pour la gestion des risques est un effort important, mais insuffisant pour assurer son efficacité. La gestion des risques est une activité qui demande un certain apprentissage, car elle demande une façon de penser qui n'est pas tout à fait naturelle dans un contexte d'affaires où la prudence est souvent perçue comme de la résistance plutôt que de la vigilance. Il est donc primordial de s'assurer que la culture de l'entreprise ou de l'unité d'affaires soit propice pour ce genre d'exercice. Sinon, l'exercice de gestion des risques sera futile. ■

(A) AUBERT, B.A., PATRY, M., RIVARD, S. (2001). « MANAGING IT OUTSOURCING RISK: LESSONS LEARNED ». CIRANO, CAHIER SCIENTIFIQUE NO.2001S-39. [HTTP://WWW.CIRANO.QC.CA](http://www.cirano.qc.ca)

(B) BERNARD, J.G., RIVARD, S., AUBERT, B.A. (2002). « L'EXPOSITION AU RISQUE D'IMPLANTATION D'UN ERP: ÉLÉMENTS DE MESURE ET D'ATTÉNUATION ». HEC MONTRÉAL, CAHIER DE LA CHAIRE DE GESTION STRATÉGIQUE DES TECHNOLOGIES DE L'INFORMATION NO.02-06. [HTTP://WWW.HEC.CA/CHAIREGESTIONTI/CAHIERSCHAIRE.HTML](http://www.hec.ca/chairegestionti/cahierschaire.html)

(C) AUBERT, B.A., BERNARD, J.G. (EDS.) (2004). « MESURE INTÉGRÉE DU RISQUE DANS LES ORGANISATIONS ». PRESSES DE L'UNIVERSITÉ DE MONTRÉAL, MONTRÉAL, QC.

La gestion des risques est une activité qui demande un certain apprentissage, car elle demande une façon de penser qui n'est pas tout à fait naturelle dans un contexte d'affaires où la prudence est souvent perçue comme de la résistance plutôt que de la vigilance.

Lectures complémentaires

Le facteur humain . . . gestion du risque ou risque de gestion

Le facteur humain est toujours un élément critique dans le déroulement de tous projets. Sa prise en compte et sa gestion sont des impératifs aussi critiques que stratégiques.

<http://www.directioninformatique.com/DI/client/fr/DirectionInformatique/Nouvelles.asp?id=40416>

L'analyse de risque, un élément fondamental de la sécurité informatique

Trop souvent négligée, particulièrement par la PME, l'analyse de risque n'en constitue pas moins un outil essentiel dans la chaîne de la sécurité informatique.

<http://www.directioninformatique.com/DI/client/fr/DirectionInformatique/Nouvelles.asp?id=35852>

Cet article de Bouchaib Bahli et Suzanne Rivard, que l'on retrouve sur le site de la Chaire de gestion en TI de HEC Montréal (<http://neumann.hec.ca/chairegestionti/cahiers/cahier0204.pdf>) analyse particulièrement le risque associé à l'impartition de l'exploitation des TI.

Le Centre de la sécurité des des télécommunications du Canada a de son côté publié un Guide de la gestion des risques d'atteinte à la sécurité des technologies de l'information (<http://www.cse-cst.gc.ca/publications/gov-pubs/itsg/mg2-e.html>).

Un autre guide qui peut être inspirant est celui produit par le National Institute of Standards and Technology du ministère américain du Commerce, le Guide de gestion du risque pour les systèmes de technologies de l'information (<http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>)

La firme spécialisée Infosec Technologies, offre une page (<http://www.infosec-technologies.com/RiskManagementResources.htm>) de liens assez exhaustive en matière de gestion des risques en TI. ■

