Septembre 2008

Méthodologie de gestion du risque informatique pour les Directeurs des Systèmes d'Information : un levier exceptionnel de création de valeur et de croissance

Sommaire

Introduction

Le risque fait partie intégrante des activités des entreprises, et sur un marché dynamique et désormais mondialisé, où règnent le changement et les incertitudes, il connaît un développement accéléré. Les acquisitions d'entreprises, les partenariats basés sur la collaboration, l'intégration mondiale et les évolutions technologiques incessantes sont autant de facteurs de risque. Aujourd'hui, les entreprises les plus performantes ont parfaitement compris comment les absorber et les limiter au mieux. Plutôt que de se contenter de traverser ces changements majeurs, elles en tirent parti et les suscitent même parfois pour créer de nouveaux potentiels. Cette résilience est un véritable levier de croissance et de profitabilité durables.

Dans un contexte marqué par l'omniprésence de l'informatique au cœur de toutes les activités d'une entreprise, la capacité d'adaptation repose de plus en plus sur l'aptitude à gérer efficacement les risques auxquels sont exposés l'informatique, l'infrastructure physique et les processus métier d'une organisation. Rien d'étonnant par conséquent à ce que, pour les DSI les plus performants, la gestion du risque constitue bien plus qu'une thématique dominante. C'est une véritable exigence qu'ils partagent au sein de l'entreprise, avec leurs homologues responsables de lignes d'activités. Pourtant, le périmètre d'influence de la plupart des DSI en matière de gestion du risque reste trop souvent limité pour conduire à un véritable gain de valeur pour l'entreprise. Force est de constater qu'en matière de risque, les DSI ont plutôt tendance à pratiquer l'évitement que la gestion. Ce qui veut dire que lorsqu'ils se concentrent trop exclusivement sur les menaces informatiques, en oubliant le rapport risques/bénéfices pour l'entreprise toute entière, ils réduisent eux-mêmes la puissance de ce levier en matière de résultats opérationnels et financiers.

Dans le contexte actuel marqué par une extrême interdépendance des activités, les responsables informatiques se doivent de percevoir et de maîtriser les avantages qu'offre la prise de risque en matière d'investissements et de gains financiers. En considérant le risque sous un angle plus global et élargi, ils peuvent percevoir l'impact des processus informatiques et de l'infrastructure sur les activités métier. Par ailleurs, ils sont en meilleure position pour exploiter les capacités de l'informatique afin de limiter les risques qui pèsent sur l'entreprise et de capitaliser sur de nouveaux potentiels de profit.

Points clés

Le périmètre d'influence de la plupart des DSI en matière de gestion du risque reste trop souvent limité pour conduire à un véritable gain de valeur pour l'entreprise.

En adoptant des principes directeurs de gouvernance centrés sur le risque, l'entreprise peut élargir sa vision et apporter à ses dirigeants une vue plus complète des risques et des bénéfices potentiels. Disposant ainsi d'enseignements très larges, ils sont à même de prendre des décisions pertinentes, axées sur l'optimisation du potentiel de chiffre d'affaires et l'acceptation d'un certain degré d'exposition au risque. Par ailleurs, ils sont en meilleure position pour mettre en place des processus d'analyse et d'automatisation efficaces, capables de prendre en compte les risques du moment, tout en protégeant les enjeux futurs de l'entreprise. Pour résumer, les DSI sont idéalement placés pondérer le rapport risques/bénéfices.

Lorsque les DSI parviennent à communiquer sur l'importance de la gestion des risques pesant sur l'informatique et l'infrastructure physique de l'entreprise, ils deviennent les promoteurs d'une nouvelle vision du risque auprès des autres responsables, et même, au final, dans l'entreprise toute entière. Mais au-delà de ce rôle éminent, ils doivent se montrer capables de transformer la démarche traditionnelle de gestion du risque informatique en un potentiel incontournable de valeur.

Valoriser les potentiels inexploités de la gestion du risque informatique

Dans un contexte instable et en évolution permanente, la prise de risques et l'aptitude à limiter leurs effets sont stratégiques pour la croissance de l'entreprise.

Lancer de nouveaux produits ou investir dans des idées novatrices représente un certain risque. Mais en cas de réussite, comme en témoignent de nombreuses entreprises du secteur de la pharmacie et de la finance, les bénéfices sont énormes. Les entreprises capables d'innover savent que le risque est un véritable levier pour la croissance de leurs activités. C'est pourquoi, plutôt que d'écarter le danger, ces firmes privilégient le développement, dans un environnement pourtant marqué par l'incertitude des résultats. Elles adoptent donc une approche adaptée pour limiter l'éventualité d'un échec.

Un nouveau rôle pour les DSI : gestionnaires du risque

Lorsque des démarches de gestion du risque concernant l'informatique et les infrastructures sont engagées, c'est rarement dans l'idée d'en faire un levier de compétitivité pour l'entreprise. Il y a différentes raisons à cela, mais qui tiennent pour l'essentiel aux limites de la démarche des dirigeants informatiques pour cerner le risque et y répondre. Si vous considérez la gestion du risque informatique exclusivement en termes de silos d'informations et de ressources, vous vous empêchez d'appréhender de manière globale les activités métier et le chiffre d'affaires de l'entreprise.

De même, au lieu de tirer parti des obligations réglementaires imposées à l'entreprise comme un bouclier contre des menaces effectives, elles sont traitées comme une simple liste de contrôle des opérations informatiques à exécuter. Toujours selon cette démarche limitée, les évolutions apportées à l'informatique, par exemple la virtualisation et les services partagés, sont perçues comme des solutions à des problèmes techniques, sans aucune prise en compte de l'impact sur l'entreprise.

D'une manière générale, les DSI considèrent la stabilité opérationnelle, la disponibilité des équipements, la protection des informations et les plans de reprise d'activité comme l'ultime objectif de la gestion du risque informatique. Même si ces actions sont bien entendu excellentes pour une gestion efficace du risque informatique, le rôle qu'elles jouent dans les processus métier ne doit pas pour autant être éludé. Il est fréquent que les responsables informatiques ne perçoivent pas jusqu'où ces actions protègent l'entreprise. Ils ne prennent pas non plus la pleine mesure du véritable filet de protection qu'ils offrent, et qui permet à l'entreprise de s'ouvrir à de nouveaux marchés, d'engager des partenariats mondiaux et de se développer. Ils ne sont tout simplement pas accoutumés à remettre l'informatique dans la perspective d'une démarche privilégiant la réduction du risque pour l'entreprise ou la création de nouveaux potentiels de chiffre d'affaires. À y regarder de plus près, l'informatique a toujours été considérée comme un centre de coûts. Avec la pression croissante qui pesait sur la réduction des coûts informatiques, les DSI ont eu davantage tendance à utiliser la gestion du risque informatique pour contenir leurs coûts qu'à mettre en place des actions novatrices axées sur la réduction des coûts d'exploitation et des risques.

Vu sous cet angle, il semble difficile pour les DSI de considérer l'informatique comme un levier de croissance pour l'entreprise. D'autre part, si elle perdure, cette approche peut conduire à écarter des potentiels de croissance pourtant pertinents, la plupart du temps pour des raisons de surestimation des risques associés. L'immobilisme lié à cette vision est un véritable problème dans un contexte marqué par les changements accélérés et des activités intégrées mondialement. Selon l'enquête « IBM Global CEO 2008 : opportunités pour le DSI », les PDG, ainsi que d'autres hauts dirigeants d'entreprises, expriment leurs préoccupations quant à l'immobilisme, dans le contexte actuel.[2] La capacité à exploiter des potentiels à l'échelle de la planète ne repose que sur la détermination à conduire le changement, et pas seulement à y réagir. La prise de risque est d'abord une question de motivation.

Qui se trouve aux avant-postes en matière de gestion du risque ?

Malgré le peu d'enclin des informaticiens pour la prise de risque, les DSI sont de plus en plus aux commandes de la gestion du risque à l'échelle de l'entreprise. Selon l'enquête « IBM Global CFO Study 2008 »,[1] 25 % des directeurs financiers, comme d'autres hauts responsables financiers, indiquent que les directeurs des systèmes d'information sont en meilleure position pour maîtriser les risques, après les directeurs financiers et les PDG. L'enquête indique toutefois que la proportion de directeurs financiers et de PDG occupant un rôle prépondérant dans ce domaine ira en décroissant au cours des trois prochaines années. Les directeurs financiers verraient bien les DSI prendre la relève.

Points clés

En adoptant une approche globale de la gestion du risque, les directeurs des systèmes d'information disposent d'une vue unifiée des menaces qui pèsent sur l'entreprise et de leurs conséquences.

Percevoir le risque d'un point de vue global

Du fait de l'omniprésence de l'informatique dans la plupart des activités des entreprises, il va sans dire que les risques auxquels s'expose une organisation découlent de ceux liés à l'informatique et à l'infrastructure physique associée. Les hauts dirigeants des entreprises sont de plus en plus conscients de la nécessité d'une meilleure gestion du risque informatique. Selon l'étude « IT Governance Global Status Report – 2008 » menée par l'ITGI (IT Governance Institute), 62 % des PDG et des DSI interrogés ont pris, en 2007, des mesures destinées à améliorer la gestion des risques, contre 45 % en 2005 et 18 % en 2003.[3]

Il n'en reste pas moins qu'aborder la gestion du risque informatique sous l'angle des silos d'informations rend plus difficile la moindre évolution réelle. Culturellement, les risques informatiques sont répertoriés en catégories strictes et donc abordés, par exemple, en termes de disponibilité des systèmes, de sécurité des accès et de plan de reprise d'activité. Cette vision analytique élude les relations d'interdépendance, ce qui peut provoquer un défaut d'appréciation du risque global auquel une activité ou un processus métier peut être exposé. L'importance de cet aspect va bien au-delà des enjeux de protection. Il a un impact important sur la croissance de l'entreprise. Prenons l'exemple d'une mise à niveau technologique destinée à faciliter le développement d'une banque à l'échelon mondial. Si l'on perçoit le risque informatique en termes de silos d'informations, il est strictement impossible pour les responsables métier de comprendre la réalité des menaces potentielles qui pèsent sur les actifs de la société. En outre, aucune mise en perspective ne permet de relier les besoins de l'entreprise en termes de compétitivité et de résilience et leurs fonctionnalités associées en termes de ressources informatiques et d'infrastructure. Une entreprise se doit donc de disposer d'une vue globale et unifiée de l'ensemble des risques auxquels elle doit faire face, sans exception.

Lorsqu'ils sont capables d'envisager le risque globalement, les responsables informatiques sont mieux à même de percevoir le lien avec les activités métier. Disposant ainsi d'un point d'observation omnidirectionnel, ils sont dans une position idéale pour maîtriser l'ensemble des menaces potentielles qui pèsent sur l'activité. Ils savent dans ce cas réagir à ces menaces (catastrophes naturelles, actes malveillants, accidents et désordre opérationnel), tout en percevant simultanément l'ensemble des conséquences éventuelles pour les actifs et les ressources de l'entreprise (personnel,

Points clés

informations, matériels, logiciels et installations physiques). Par ailleurs, ils prennent mieux la mesure de la dynamique du risque, en étant absolument conscients que des enjeux de stabilité opérationnelle en apparence négligeables, par exemple des capacités insuffisantes, sont susceptibles de se transformer en pertes lourdes s'ils ne sont pas maîtrisés. Par leur parfaite connaissance des systèmes sur lesquels reposent chacune des activités métier, les DSI maîtrisent davantage les délais de reprise de l'exploitation en fonction de critères de priorités. Par ailleurs, ils identifient plus facilement les moyens et l'échelonnement nécessaires aux évolutions de l'informatique. Et c'est parce qu'ils connaissent l'effet de levier pour l'entreprise des actions de réduction du risque informatique qu'ils sont les mieux placés pour promouvoir la démarche auprès de la direction.

Remettre à plat l'ensemble de la gestion du risque informatique

En adoptant une approche globale de la gestion du risque, les directeurs des systèmes d'information disposent d'une vue unifiée des menaces qui pèsent sur l'entreprise et de leurs conséquences.

Manifestement, les DSI sont appelés à adopter une approche élargie et orientée métier de la gestion du risque informatique. Au final, il s'agit bien d'un élément essentiel de la mise en cohérence stratégique de la fonction Informatique et de l'entreprise. En effet, elle exige des DSI qu'ils assument leurs fonctions en termes de rapport risques/bénéfices, qui est bien le langage qu'emploie le comité de direction.

Une approche orientée métier considère les défis relatifs à la gestion du risque informatique sous l'angle des processus métier. Il s'agit, dans ce cadre, d'identifier les risques en corrélant les processus de l'entreprise et les risques potentiels liés à l'informatique. L'analyse des dépendances permet ainsi d'identifier les modalités d'interaction entre les activités métier et des éléments spécifiques de l'informatique et de l'infrastructure de l'entreprise. En structurant ensuite les activités informatiques en différentes couches, il est plus facile de revenir aux causes sous-jacentes relevant de l'informatique.

L'analyse des dépendances permet de mieux comprendre, avant leur apparition, l'origine informatique des problèmes potentiels que peut rencontrer l'entreprise.

Une des approches consiste à évaluer les risques informatiques en termes de processus métier et de résultats. Les résultats métier et leurs risques associés sont identifiés pour chaque processus informatique. Prenons comme exemple une action de conduite du changement. Dans ce cas, le changement peut concerner la technologie (consolidation des centres informatiques, nouvelles configurations), mais aussi des évolutions des activités métier (opérations d'acquisitions, rationalisation des coûts). Les risques envisageables dans ce contexte portent sur les durées d'arrêt des systèmes, les pertes d'informations, les retards de traitements système et les capacités insuffisantes des ressources. Pour l'entreprise, ces résultats sont tous représentatifs de problèmes de prise en charge par l'informatique, qu'il s'agisse d'une

planification inadaptée, d'un besoin de déploiement rapide ou de l'absence de réactivité. Il est possible d'en trouver la cause dans une conception incorrecte des processus, mais aussi dans une réalisation inadaptée (parfois liée à des problèmes de formation), ou encore dans une réaction inappropriée face à un problème. L'essentiel est de revenir à l'origine d'une situation néfaste pour l'entreprise, et en particulier, de mettre en lumière les causes profondes reposant sur les processus.

Les avantages des approches fondées sur les processus pour la gestion du risque informatique

En adoptant des approches basées sur les processus, les entreprises mettent davantage en lumière leurs lacunes et la nécessité d'aller plus loin en matière de gestion du risque informatique. Selon l'étude « IT Governance Global Status Report – 2008 », les PDG et les DSI qui ont implémenté la méthodologie COBIT au sein de leurs entreprises avaient davantage tendance à considérer la gestion du risque informatique comme « très importante » par rapport aux autres dirigeants interrogés (57 % contre 44 %). Par leur démarche plus déterminée en la matière, ces entreprises tendent naturellement à dynamiser la création de valeur métier.

Un cadre structuré de gouvernance est d'une importance stratégique

Sans un cadre robuste de gouvernance, il n'y a pas de gestion du risque satisfaisante. Ce cadre permet de mettre en place les politiques, les contrôles et les règles opérationnelles qui permettent aux responsables informatiques de gérer les risques et de pondérer leur valeur pour l'entreprise. Toutefois, pour être efficace à long terme, un cadre de gouvernance doit s'adapter au contexte évolutif dans lequel opère une entreprise. Des principes de gouvernance extrêmement sophistiqués existent déjà. Les DSI pourront donc tirer un profit immédiat des règles et « meilleures pratiques » déjà proposées en matière de gestion du risque informationnel.

L'ITGI (IT Governance Institute) a développé d'excellents principes de gouvernance, généralement appliqués dans le monde entier et basés sur des standards ouverts. De son côté, la méthodologie COBIT (Control Objectives for Information and related Technology) propose un ensemble de bonnes pratiques, centrées sur la gouvernance en matière de technologie et d'infrastructures, et qui englobent la gestion du risque. La spécificité de la démarche COBIT est de se placer dans une perspective d'exécution. Pour sa part, la méthodologie Val IT de l'ITGI est plus axée sur la maîtrise des investissements d'entreprise fondés sur l'informatique, gestion du risque comprise, avec pour objectif d'optimiser le retour sur investissements.[4] Par ailleurs, l'ISO (Organisation internationale de normalisation) et l'Office public britannique du Commerce, avec la méthodologie ITIL (IT Infrastructure Library), ont développé des principes directeurs particulièrement utiles en matière de gestion du risque informatique. IBM, de son côté, a réalisé la synthèse de ces bonnes pratiques en proposant les méthodologies PRM-IT (Process Reference Model for IT), CBM-BoIT (Component Business Model for the Business of IT) et Resilient Enterprise Blueprint, en y associant une feuille de route pour faciliter leur implémentation.

Au-delà d'une meilleure résilience, de la normalisation des processus métier et de la mise en place de bonnes pratiques, la gouvernance conduit aussi à une gestion plus efficace des risques affectant le chiffre d'affaires de l'entreprise. Outre une meilleure protection vis-à-vis des pénalisations dues au

Points clés

Les directeurs des systèmes d'information sont naturellement appelés à jouer un rôle de premier plan dans la mise en place de processus structurés, capables de dynamiser la réactivité des entreprises face au risque et d'améliorer leurs capacités à anticiper sur les menaces, à les analyser et à y répondre.

titre des contrats signés, des règles du secteur d'activité ou de la réglementation, elle favorise le développement de l'activité et la maîtrise des contrats existants. Une entreprise veut connaître ses capacités à assurer la continuité de ses activités, quelles que soient les menaces rencontrées. Pour leur part, les clients exigent des garanties de protection de leurs informations, mais aussi de leurs autres actifs. Un cadre de gouvernance est donc la réponse adaptée aux objectifs de gestion du risque.

Même si les normes et les démarches mises en avant par chacune de ces méthodologies diffèrent par leur terminologie, les recommandations qu'elles proposent en matière de gestion du risque informatique convergent :

- **Définir le périmètre de l'analyse du risque.** *Il s'agit d'identifier les activités métier, les initiatives et les éléments technologiques et d'infrastructure de l'entreprise qui doivent être pris en compte dans la démarche de gestion du risque informatique.*
- **Cibler et définir les risques.** *La démarche consiste à associer chacune des activités métier à des menaces possibles et à des ressources exposées à des risques.*
- **Estimer la probabilité de la réalisation d'un risque et son niveau d'impact.** *Il s'agit de calculer la probabilité et la gravité d'une atteinte aux activités métier, pour disposer, au final, d'une vision globale des risques encourus.*
- **Évaluer les mesures de contrôle.** *Il s'agit ici de mesurer la qualité des procédures de contrôle déjà en place pour prévenir, identifier et limiter les risques, en prenant en compte les coûts par rapport à la valeur créée.*
- **Apprécier le risque et élaborer les actions et les réponses correspondantes.** *L'approche consiste à analyser les risques par rapport à la volonté de l'entreprise, établir les actions prioritaires de réduction du risque et décider des investissements en fonction d'une analyse coûts/bénéfices.*
- **Mettre en œuvre des actions visant à réduire les risques.** *Cette étape consiste à développer, tester et mettre en place des plans détaillés de réponse aux risques.*
- **Assurer un contrôle et un retour d'informations permanents.** *Il s'agit ici d'assurer la collecte permanente d'informations concernant les menaces affectant la démarche de gestion du risque, son impact et son efficacité, puis d'adapter les plans d'action et les processus de gestion du risque en fonction de ces informations.*

Points clés

Des processus structurés de ce type favorisent la réactivité des entreprises et leurs capacités à anticiper sur les menaces, à les analyser et à y répondre. L'obstacle de la complexité organisationnelle peut toutefois tempérer leur mise en œuvre. La gestion du risque entre de plus en plus dans les attributions des directeurs des systèmes d'information. En outre, la plupart de ces menaces appartiennent au périmètre de contrôle de l'informatique et les DSI sont naturellement appelés à jouer un rôle de premier plan dans la mise en place de ces processus, en s'engageant dans des actions consistant à :

- *Affecter les financements et les ressources nécessaires aux démarches d'analyse du risque*
- *Proposer des orientations destinées à favoriser le dialogue entre les différents intervenants concernés et s'assurer en permanence de la cohérence entre les objectifs métier et la conformité avec les politiques de gouvernance de l'entreprise*
- *Promouvoir l'amélioration constante des processus*
- *Mettre l'accent sur l'intégration accrue de la notion de risque dans la gouvernance globale de l'entreprise*
- *Élaborer des politiques de gestion du risque destinées à accompagner les activités de l'entreprise.*

Le rôle important du personnel, de l'organisation et de l'automatisation

À l'évidence, la direction d'une entreprise ne peut que se montrer très favorable à des programmes de gestion du risque informatique capables de mettre en évidence des menaces potentielles pour ses activités, tout en proposant des réponses plus souples et moins coûteuses à ces risques. Les DSI ont ici une opportunité exceptionnelle de réaliser ces objectifs en levant les obstacles liés au personnel, à l'organisation et à l'automatisation :

L'efficacité des démarches de gestion du risque informatique repose à la fois sur une culture centrée sur le risque, sur une détermination sans faille des dirigeants de l'entreprise et sur des processus automatisés destinés à faciliter l'analyse et la résolution des problèmes.

- **Personnel.** *Pour être véritablement efficace, la gestion du risque doit dépasser les limites d'un simple programme. Elle doit s'intégrer profondément dans l'état d'esprit du personnel de l'entreprise. Une entreprise a l'obligation de développer une vraie culture centrée sur le risque, adaptée au large éventail de menaces auxquelles elle a à faire face, mais en y adjoignant une stratégie de réponse pour les limiter. Plutôt que de privilégier la réaction après coup, les programmes de formation en la matière doivent préparer les collaborateurs de l'entreprise à détecter et identifier les risques, et à y répondre. Chacun des employés d'une entreprise doit se sentir véritablement partie prenante de la protection de l'entreprise et de la création de valeur.*

Points clés

- **Organisation.** *Si le soutien de la direction à la gestion du risque informatique va de soi, l'efficacité de la démarche nécessite des approches complémentaires. Les processus de gestion du risque, notamment ceux que décrit la méthodologie* COBIT*, doivent s'accompagner de procédures concernant la continuité de l'activité et de principes de gouvernance centrés sur le risque, selon une approche descendante. La démarche nécessite une intégration stratégique dans la fibre même de l'entreprise, et ceci, afin de décompartimenter les sources de risques et de maîtriser complètement les dépendances et les ruptures d'exploitation potentiellement néfastes pour l'activité.*
- **Automatisation** *L'automatisation facilite la gestion du risque informatique selon deux axes importants. Elle permet tout d'abord de réduire la complexité de l'analyse et de la diffusion d'informations concernant les risques stratégiques. En effet, plus la taille d'une entreprise est importante, ce qui induit davantage encore d'évolutions métier et technologiques, plus les processus mis en jeu sont complexes. Deuxièmement, l'automatisation facilite l'évaluation et la réduction des risques en conditions réelles. L'utilisation d'applicatifs de gestion des activités métier et des services, de suivi des procédures de contrôle et de supervision de la sécurité permet de limiter la mise à contribution des ressources, grâce à des diagnostics d'analyse de cause à effet et des fonctions d'identification et de réaction (sense-and-respond). L'entreprise peut ainsi plus facilement identifier les risques, déclencher des procédures anticipées, mais aussi simplifier les réponses et en réduire les coûts, et enfin, rationaliser les processus de gestion du risque.*

C'est en harmonisant le niveau de réponse au risque du personnel de l'entreprise, de l'organisation et des processus automatisés qu'une entreprise peut tirer davantage de valeur métier de ses initiatives de gestion du risque.

C'est sur ces domaines que les entreprises doivent faire porter leurs efforts, tout en pondérant de manière permanente leur impact pour une gestion efficace du risque informatique. Une démarche de sensibilisation au risque à l'échelle de l'entreprise par exemple, peut être renforcée par une formation interne. Cependant, une fois réalisée, cette formation ne donnera pas pour autant aux employés de l'entreprise les processus nécessaires pour une action sur le terrain. À l'inverse, le personnel formé aux processus de réponse au

Points clés

risque ne seront pas à même d'apporter de véritables solutions à des problèmes sans une certaine automatisation. Tout déséquilibre en termes de qualité de réponse dans ces trois domaines conduit à un niveau insuffisant de création de valeur par rapport aux investissements réalisés. C'est en améliorant en permanence son approche dans les trois domaines qu'une entreprise peut obtenir les meilleurs résultats.

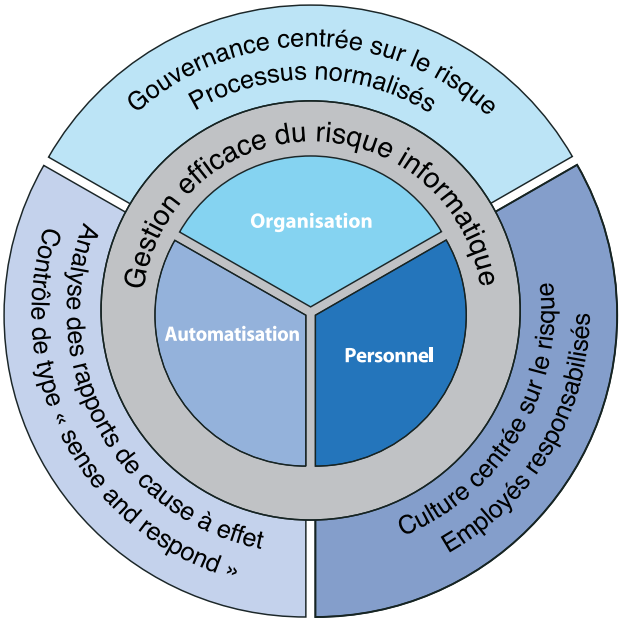

Figure 1. L'efficacité de la démarche de gestion du risque repose sur l'harmonisation des investissements dans le personnel, l'organisation et l'automatisation.

Optimiser le rapport risques/bénéfices : le rôle stratégique des DSI

Aujourd'hui, les directeurs des systèmes d'information se doivent de considérer la gestion de l'informatique comme un levier d'optimisation de la création de valeur, intégrant la limitation de la prise de risque.

Compte tenu du rôle toujours plus stratégique des DSI au sein du comité de direction, les attentes en matière de gestion du risque informatique sont plus élevées que jamais. Les directeurs des systèmes d'information se doivent de maîtriser le coût réel des risques informatiques, ce qui signifie qu'ils doivent connaître parfaitement l'impact de leurs décisions sur le chiffre d'affaires, la fidélisation des clients et la compétitivité. Dans un monde orienté sur la création de valeur, la gestion informatique doit se concentrer sur la réalisation du meilleur résultat en limitant au maximum les risques (figure 2). C'est ici qu'intervient la notion de budgétisation du risque.

Points clés

Grâce à cette démarche, les DSI sont à même d'optimiser les bénéfices pour l'entreprise en investissant leur capital de risque de la manière la plus efficace possible.

Mettre en place un budget de risque

La budgétisation du risque consiste à créer un cadre permettant de définir les risques qu'il est possible de prendre, compte tenu des enjeux. Similaire à celle des responsables financiers, l'approche consiste à affecter des ressources suffisantes pour répondre à des risques informatiques « identifiés », concernant, par exemple, la disponibilité de services. Par ailleurs, les DSI doivent provisionner un budget plus important lorsque les risques encourus sont véritablement inconnus. Considérons par exemple la création d'un nouveau portail destiné à réduire la perte de clientèle, ou la mise en place de capacités largement suffisantes pour répondre à des volumes de transactions prévisionnels pour un produit nouveau. Les différentes étapes mises en œuvre pour réduire les risques informatiques rencontrés sont plus facilement maîtrisables que le taux d'acceptation réel par les clients d'un produit récemment lancé ou l'efficacité d'un nouveau circuit de distribution. Grâce à la budgétisation du risque, les DSI peuvent prendre des décisions justifiées, de concert avec les responsables métier, pour affecter des ressources et optimiser ainsi les résultats de l'initiative. En utilisant leurs ressources de manière avisée, les directeurs des systèmes d'information évitent aux responsables métier d'utiliser leur budget de risque sur d'autres postes, plus difficiles à gérer, dans le cadre d'une nouvelle action.

Ouvrir le débat sur le risque

C'est un fait, les managers n'aiment pas parler du risque. Il est évidemment plus facile et moins perturbant d'en rester à l'idée que les projets se dérouleront comme prévu et qu'aucun incident ne viendra les bouleverser. Dans une telle atmosphère d'évitement, les collaborateurs de l'entreprise sont très naturellement peu enclins à faire remonter les problèmes susceptibles d'avoir un impact important sur un projet. Ils attendent souvent trop longtemps, en prenant tardivement en compte les risques alors qu'une solution informatique se trouve déjà en production, et ils deviennent malgré eux les héros du moment. Lorsqu'une entreprise persiste dans ce type de culture, elle se trouve obligée de réagir aux problèmes lorsqu'ils apparaissent, et bien souvent dans une situation de crise.

Points clés

L'entreprise attend des DSI qu'ils se tournent vers leurs collègues pour lesquels le risque est une priorité et qu'ils démontrent que l'informatique peut répondre de manière anticipée à un risque, tout en dynamisant la création de valeur.

La plupart des DSI ont suffisamment d'expérience en matière de gestion de projet pour savoir que des « projets sans risques » n'existent tout simplement pas. Ils sont parfaitement conscients qu'il est plus efficace d'anticiper sur les éventuels problèmes que d'attendre de devoir y réagir. En dialoguant avec d'autres dirigeants pour lesquels le risque est une notion prioritaire (directeurs financiers, directeur de la gestion des risques, responsables de la continuité de l'activité), les DSI peuvent mieux sensibiliser l'entreprise à la notion de risque et favoriser une culture positive qui encourage un retour d'information rapide. Amenés à collaborer avec des responsables de lignes d'activité, et même des intervenants extérieurs (investisseurs, fournisseurs, clients, organismes d'évaluation de solvabilité, organismes de tutelle), les directeurs des systèmes d'information sont en position idéale pour promouvoir les modalités d'une collaboration orientée sur la réduction du risque informatique, et mieux encore, pour indiquer comment l'informatique peut anticiper sur les risques et dynamiser la création de valeur.

Construire un argumentaire pour une gouvernance centrée sur le risque

Une gouvernance centrée sur le risque doit permettre d'intégrer des équipes à l'échelle de l'entreprise et de responsabiliser chacun vis-à-vis des notions de risque et de résilience.

Pour assurer une gestion du risque sans discontinuités et orientée sur l'anticipation, une gouvernance centrée sur le risque est indispensable. Quelle que soit sa forme, la gouvernance centrée sur le risque permet aux dirigeants de l'entreprise de disposer d'une vision plus globale en la matière, en intégrant les équipes chargées de ce domaine à l'échelle de toute l'entreprise et en responsabilisant chacun aux notions de risque et de résilience. Parce qu'ils comprennent les dépendances organisationnelles génératrices de risque, les collaborateurs de l'entreprise sont mieux à même de prendre des décisions courantes susceptibles d'influer positivement sur les risques auxquels l'entreprise est exposée. Par ailleurs, les responsables de lignes d'activité voient plus loin que les problématiques de leurs propres organisations, et ils disposent des moyens de gérer les priorités de leurs investissements et de privilégier les meilleures réponses pour l'entreprise. Les méthodologies COBIT et Val IT, entre autres, permettent d'accompagner et de contrôler ces décisions, par des moyens spécifiques d'analyse du risque en fonction des bénéfices potentiels.

Points clés

Les DSI jouent un rôle essentiel auprès des responsables des lignes d'activité pour promouvoir les avantages d'une vision consolidée du risque et combler les lacunes de dialogue et d'action en matière de risque.

Une gouvernance centrée sur le risque permet aux dirigeants de l'entreprise d'utiliser la gestion du risque informatique comme un levier de résilience, mais aussi comme un bouclier de protection de la technologie et de l'infrastructure physique, et donc au final, comme un facteur de dynamisation de la croissance. Les DSI ont manifestement tout intérêt à promouvoir cette vision de la gestion des risques pesant sur l'informatique et l'infrastructure physique associée. En première approche, leur démarche consiste à éliminer les différents silos informatiques générateurs de risques et à proposer une vision unifiée pour mettre en lumière les interdépendances fonctionnelles et l'ensemble des menaces et des impacts potentiels sur l'activité, la technologie et l'infrastructure.

Ensuite, les DSI doivent étendre la logique globale de gestion du risque au reste de l'entreprise, en aidant les responsables de lignes d'activité à comprendre l'ensemble des risques auxquels sont exposés leurs propres processus. La plupart d'entre eux ne sont tout simplement pas conscients des risques liés aux autres secteurs, ou de ceux qu'eux-mêmes font courir aux autres. Une vision globale est donc absolument essentielle, car c'est la seule capable de révéler les niveaux d'exposition stratégiques, les pertes réelles et les tendances. Par ailleurs, la démarche permet de simplifier le processus, parce qu'elle élimine, de fait, toute discussion particulière concernant des risques spécifiques à un secteur.

En ce qui concerne la direction, qui doit rendre des comptes aux actionnaires et aux administrateurs, l'importance d'une vision consolidée du risque est essentielle et les DSI ont un apport important dans la précision de cette vision unifiée. Lorsqu'il s'agit par exemple, pour les directeurs financiers, d'évaluer les points positifs de projets ou d'investissements nouveaux, les DSI jouent un rôle essentiel pour mettre en lumière les risques dans les calculs de rapport risques/bénéfices de la direction financière. Les directeurs des systèmes d'information peuvent également mettre en avant le fait que la réduction du risque informatique se traduit par une meilleure stabilité opérationnelle, et au final, par une plus grande stabilité financière.

Points clés

Les DSI disposent des connaissances applicatives et des informations nécessaires pour simplifier l'analyse, le contrôle et les réponses aux situations de risque.

Les DSI savent parfaitement que des applications appropriées peuvent simplifier l'analyse et le contrôle du risque, et qu'ils disposent de l'expertise pour les déployer. Les applications d'analyse de dépendances peuvent faciliter l'identification d'éventuels domaines ponctuels de défaillance et des conflits éventuels de partage des ressources. Ils peuvent également aider les responsables de lignes d'activité à mieux comprendre l'origine possible des risques, mais aussi à en identifier les profils, puis à tirer parti de leurs capacités d'anticipation. C'est un fait que les dépendances globales liées aux activités, aux processus et aux applications métier n'apparaissent pas clairement pour les responsables d'activité. C'est pourquoi les DSI ont un rôle stratégique à jouer pour mettre en évidence ces dépendances à l'échelle de l'entreprise toute entière. Pour ce faire, ils peuvent utiliser des techniques de prédiction, destinées à prévoir les risques, et non se contenter de réagir aux problèmes. En outre, leur connaissance des méthodologies d'optimisation des processus, comme Six Sigma, peut également apporter beaucoup en matière de réduction des risques tout en favorisant la mise en place d'un langage commun avec les lignes d'activité, éventuellement déjà utilisatrices de ces applications.

Éliminer la complexité

La complexité des infrastructures et des applications est une source de risques supplémentaires sans contrepartie en termes d'avantages métier.

Les grandes infrastructures informatiques et physiques sont souvent complexes, mais la plupart d'entre elles sont tout simplement devenues inextricables. C'est le cas, par exemple, d'une infrastructure courante, basée sur une multiplicité de plates-formes hétérogènes, et mise en œuvre pour satisfaire des préférences individuelles plutôt que pour répondre à des exigences métier spécifiques. Ces infrastructures se caractérisent non seulement par des délais de réaction accrus et des ressources nécessaires plus volumineuses, mais aussi par des risques supplémentaires sans contrepartie indiscutable en termes d'avantages métier. S'agissant d'applications complexes, l'effet produit est le même, parce qu'il conduit à accroître la charge de gestion nécessaire sans apporter de valeur.

Les DSI paient souvent le prix fort de la complexité informatique, mais aussi des risques qui en résultent. C'est évidemment eux qui manifestent la plus grande motivation à s'engager dans la simplification des infrastructures. Qu'il s'agisse de consolidation et de virtualisation ou encore des architectures orientées service (SOA), lorsque les DSI s'engagent dans des actions visant à améliorer le retour sur investissement, ils adoptent tout naturellement une approche visant à éliminer la complexité.

Points clés

Créer un environnement favorisant la création de valeur basée sur la gestion du risque informatique
✓ Mettre en place une vision unifiée et globale de la gestion du risque en reliant les silos de gestion du risque entre l'informatique et l'entreprise
✓ Sensibiliser l'entreprise à l'ensemble des menaces potentielles et à tous leurs effets possibles sur les actifs et les ressources
✓ Se servir du levier de l'analyse des dépendances pour mettre en lumière les interconnexions fonctionnelles et les rapports de cause à effet des risques
✓ Tirer parti des méthodologies, des standards ouverts et des bonnes pratiques en matière de gestion du risque informatique, au moyen de cadres de gouvernance structurés
✓ Améliorer la gestion du risque informatique par des évolutions maîtrisées au niveau du personnel, de l'organisation et de l'automatisation
✓ Établir un budget de risque, en affectant un capital de risque basé sur des bénéfices potentiels
✓ Mettre en relation de manière périodique les responsables métier et les partenaires externes de l'entreprise pour éliminer les barrières culturelles et faire progresser les échanges en matière de gestion du risque
✓ Promouvoir l'importance d'une gouvernance centrée sur le risque
✓ Éliminer les éléments de complexité de l'informatique et de l'infrastructure susceptibles d'augmenter l'exposition au risque et de réduire les bénéfices

Figure 2. Actions d'amélioration des performances en matière de rapport risques/bénéfices – ensemble d'actions proposées aux DSI.

Au-delà des aptitudes à anticiper sur les risques pour dynamiser la croissance, la démarche de gestion du risque offre aux DSI des opportunités de progression personnelle, dans un contexte où ils sont appelés à développer de nouvelles relations, à étendre leur périmètre d'influence et à renforcer leur crédibilité au sein du comité de direction.

Utiliser le rôle stratégique des DSI pour promouvoir la gestion du risque informatique

Les directeurs des systèmes d'information ont devant eux une opportunité unique de démontrer leur leadership au niveau de l'entreprise en favorisant un meilleur impact en matière de rapport risques/bénéfices de l'informatique auprès des directeurs financiers et des responsables de lignes d'activité. Mise entre des mains compétentes, la gestion du risque informatique est un gisement exceptionnel de création de valeur, avec comme préalable la nécessité d'une mutation de l'approche traditionnelle des DSI en matière de risque, faute de quoi ils ne pourront saisir les potentiels de croissance créés. Au-delà de l'innovation et du développement du chiffre d'affaires, une gestion anticipée du risque peut être une source d'évolution personnelle, en favorisant les relations, l'influence et la crédibilité stratégique des DSI au sein du comité de direction.

Conclusion

La plupart des dirigeants d'entreprises sont conscients de la relation de cause à effet entre croissance et risque. Par leur participation de plus en plus stratégique aux décisions, les directeurs des systèmes d'information doivent dépasser la technique, bien au-delà de la simple prévention des menaces, et considérer le risque dans une perspective davantage globalisée et centrée sur les activités métier, avec pour finalité, la création de potentiels. L'entreprise attend des DSI qu'ils cessent d'aborder la gestion du risque en termes de silos d'informations et qu'ils mettent en place une démarche axée sur la réalisation du plein potentiel de l'informatique pour la création de valeur. Par leur connaissance des applications et leur vision globale de l'entreprise, ils sont en position idéale pour aider les directeurs financiers et les responsables métier à exploiter le gisement de croissance qu'offre la gestion du risque informatique. Mieux encore, par leur démarche proactive axée sur la promotion et la mise en œuvre d'un cadre de gouvernance centré sur le risque, les directeurs des systèmes d'information sont aux avant-postes pour développer au sein de l'entreprise des leviers capables de contenir les crises, mais aussi de favoriser le profit et la création de valeur.

Pour de plus amples informations

Pour plus d'informations sur la gestion du risque informatique et la création de valeur, contactez IBM ou votre partenaire commercial IBM, ou visitez : **ibm.com**/cio/fr

IBM France
Tour Descartes – La Défense 5
2, avenue Gambetta
92066 – Paris La Défense Cedex

La page d'accueil d'IBM est accessible à l'adresse **ibm.com**/fr

[1] IBM, *Le juste équilibre entre risques et performances au sein d'une organisation financière intégrée : étude internationale sur la fonction Finance « Global CFO Study 2008 »,* octobre 2007. www.ibm.com/gbs/2008cfostudy L'étude « Global CFO Study 2008 » a été réalisée en collaboration avec la Wharton School (Université de Pennsylvanie) et l'Economist Intelligence Unit.

[2] IBM, *L'entreprise de demain : « Global CEO Study »,* juin 2008. www.ibm.com/ibm/ideasfromibm/us/ceo/20080505/index.shtml.

[3] IT Governance Institute, *IT Governance Global Status Report – 2008*. www.itgi.org/AMTemplate.cfm?Section=ITGI_Research_Publications&Template=/ContentManagement/ContentDisplay.cfm&ContentID=39735
La synthèse « IT Governance Global Status Report – 2008 » est basée sur une enquête internationale menée auprès de DSI et de PDG par PricewaterhouseCoopers pour l'IT Governance Institute (www.itgi.org/).

[4] Les méthodologies COBIT et Val IT, basées sur des standards ouverts, sont accessibles gratuitement auprès de l'IT Governance Institute.

CIW03045-FRFR-00