Guide de gestion des risques des projets de développement de système

Services gouvernementaux Québec

Ministère des services gouvernementaux
Juillet 2005

Table des matières

Gestion des risques

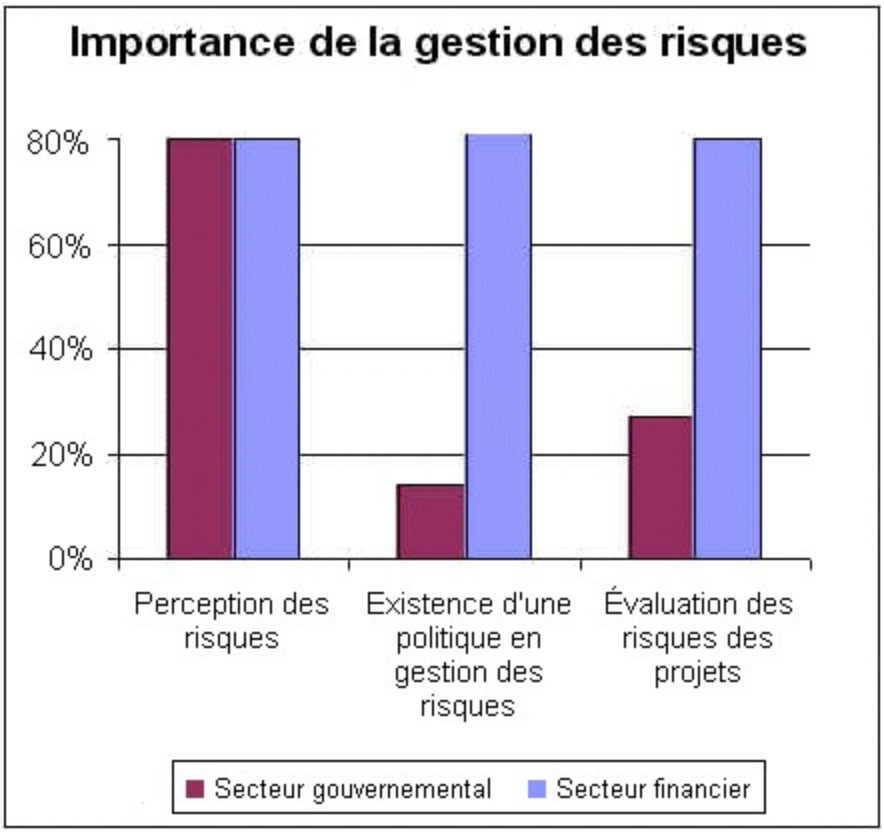
Dans les pages qui suivent, vous trouvez un exemple de gestion du risque dans le domaine du développement informatique.

1 Introduction

Dans cette section, les enjeux, coûts et bénéfices sont présentés, suivi de la définition du risque. Finalement, les principaux concepts de la gestion des risques clôtureront la section.

1.1 Enjeux, coûts et bénéfices

1.1.1 Importance des risques



Une stratégie efficace de gestion des risques fait partie des moyens importants pour permettre aux organisations d'atteindre leurs objectifs d'affaires. C'est ce qu'ont révélé 85 % des répondants lors d'un récent sondage réalisé à travers le Canada.

Ce même sondage révèle d'ailleurs que deux secteurs sont particulièrement sensibles à une gestion efficace des risques, soit les secteurs financiers et gouvernementaux. Ce sont les deux secteurs qui se considèrent les plus à risques (80 % des répondants). Au contraire du secteur financier qui est le plus sophistiqué en gestion des risques (81 % ont une politique de gestion des risques et 80 % effectuent une évaluation des risques de leurs projets), le secteur gouvernemental se considère le moins bien préparé pour gérer les risques (14 % ont une politique de gestion des risques et 27 % effectuent une évaluation des risques de leurs projets).

Parmi les sept risques les plus susceptibles de se produire, les répondants en ont identifié qui se rapportent au développement d'applications :

- ➔ risques reliés au client incluant son service et sa satisfaction;
- ➔ risques reliés à la production incluant la conception, le développement et la livraison;
- ➔ risques reliés au personnel;
- ➔ risques reliés à la technologie.

1.1.2 Enjeux

Les risques représentent un enjeu majeur pour les organisations et plus particulièrement pour les organisations qui développent des applications. Les enjeux sont de différents ordres. Mentionnons à titre d'exemples, les enjeux d'ordre :

Stratégique : Les risques peuvent mettre en péril la mission et la stratégie de l'organisation tout comme ils peuvent, s'ils sont bien gérés, permettre à l'organisation qui les coure de profiter d'opportunités d'affaires.

Financier : Il est reconnu qu'un projet dont le pourcentage de risque est élevé possède de grandes chances de ne pas rencontrer ses objectifs et ainsi de dilapider les avoirs de l'organisation si le projet s'avère un échec.

Politique : Les nouveaux programmes gouvernementaux visant à améliorer les services à la population sont très souvent dépendants de la réussite des projets informatiques. Leur échec peut avoir des impacts néfastes auprès de la population desservie par ces programmes et créer un fort mécontentement auprès de la population et des dirigeants politiques.

Administratif : Le fonctionnement d'un ministère ou d'un organisme peut être grandement perturbé par le retard d'un projet, par le dépassement de ses coûts ou par la livraison partielle ou inadéquate des fonctionnalités attendues.

Humain : Un projet informatique exige un effort soutenu, tant de la part de ceux qui participent au développement, que de la part des futurs utilisateurs. Du côté du développement, cela exige de la part du personnel un engagement de tous les instants, l'apprentissage fréquent de nouvelles méthodes ou de technologies et une capacité à travailler en équipe et sous pression. Du côté des utilisateurs, cela leur exige de s'adapter à de nouvelles façons de faire et éventuellement de changer leur milieu de travail à la suite du réaménagement de leurs tâches. La réussite des projets informatiques est donc extrêmement importante pour l'évolution des organisations. C'est pourquoi, la gestion des risques mérite une grande attention auprès de la haute direction, des informaticiens et des clients.

1.1.3 Coûts

Une question en rapport avec la gestion des risques que tout chef de projet devrait en principe se poser tout au long de son projet est : « Combien devrais-je investir dans la prévention de problèmes potentiels qui ne surviendront peut-être pas ? »

Le SEI a publié en 1994 un rapport technique concernant l'adoption de programmes visant à réduire le nombre et la fréquence des problèmes reliés au processus de développement et d'entretien d'applications (CMU/SEI-94-TR-013, ADA 283848, « Benefits of CMM-Based Software Process Improvement : Initial Results », Herbsleb, J; Carleton, A.; Rozum, J.; Siegel, J.; Zubrow, D.; Software Engineering Institute, 1994). De tels programmes visent effectivement à réduire les risques résultant de la façon dont les personnes, les procédures, les méthodes, les équipements et les outils sont intégrés dans le but de réaliser une application et désignés par le terme « risques opérationnels » ou « risques communs », par opposition aux risques intrinsèquement reliés à un produit ou à un service donné désignés par « risques spécifiques » ou « risques singuliers ».

GRafP Technologies, dans le cadre de ses activités en gestion de risques dans plus de 65 organisations, a observé que chaque risque en développement et en entretien d'applications est constitué d'une composante « opérationnelle » à 70 % et d'une composante « spécifique » à 30 %. Exprimée d'une autre façon, cette observation revient à conclure que dans un projet faisant appel aux technologies de l'information, 70 % des problèmes seront dus à des « risques opérationnels » qui se sont concrétisés et 30 % à des « risques spécifiques ». Les données compilées par le SEI à l'égard du coût de l'amélioration des processus de développement et d'entretien d'applications devraient en principe se situer entre 1 % et 3 % du budget assigné au développement et à l'entretien d'applications. Le lien existant entre la gestion des « risques opérationnels » et l'amélioration des processus de développement et d'entretien d'applications permet de déduire que les coûts associés à la gestion des risques devraient au minimum être du même ordre de grandeur.

Il est par ailleurs évident que le budget alloué à la gestion des risques sera fortement dépendant des risques encourus. Certains risques demanderont un investissement élevé en raison de l'importance de leur impact ou de la forte probabilité de survenir qui les caractérise.

Afin de déterminer plus précisément les budgets à investir dans la gestion des risques, une organisation devrait en premier lieu sélectionner un échantillon de projets récemment complétés ou en cours et inventorier les problèmes rencontrés au cours de leur réalisation. Si l'organisation a en sa possession des données numériques quant aux pertes ayant été encourues à la suite de ces problèmes, elle pourra assigner une valeur entre 25 % et 50 % des pertes à la prévention que de tels problèmes se répètent au cours des projets ultérieurs. La valeur de 50 % est suggérée s'il n'existe pas de données ou de méthode permettant de

déterminer la fréquence de ces problèmes ou la probabilité qu'ils surviennent à nouveau. Elle correspond à associer les problèmes en question à des événements aléatoires. Une valeur de 50 % des pertes, correspond donc à investir un montant égal à l'espérance de perte, alors qu'une valeur de 25 % correspond à investir un montant égal à la moitié de l'espérance de perte. Une valeur inférieure à 25 % n'est pas recommandée initialement car elle correspond essentiellement à une attitude de prise de risque. Si l'organisation n'est pas en mesure de compiler la valeur des pertes encourues, elle devra poser la question « Quel montant l'organisation aurait-elle été disposée à défrayer pour que les problèmes ne surviennent pas ou qu'ils surviennent avec un impact réduit ? ».

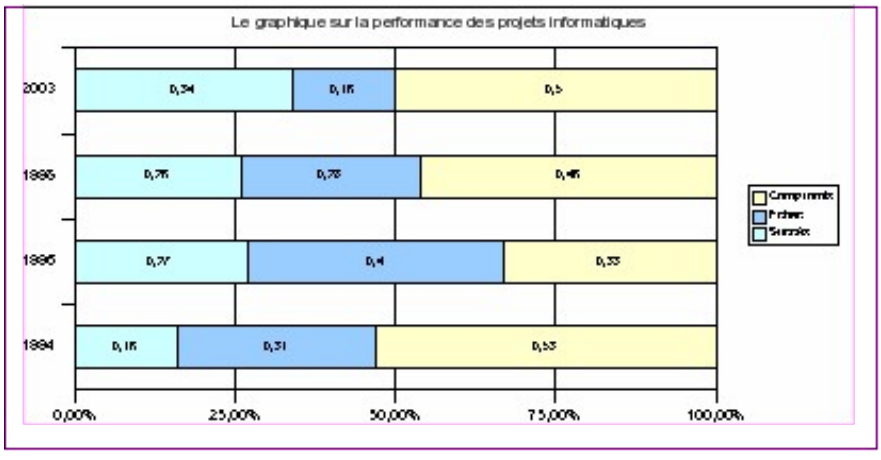
Certaines pertes encourues au cours de la réalisation d'un projet sont mesurables mais il est difficile voire impossible de leur assigner une valeur monétaire (les échecs en technologies de l'information font rarement l'objet d'une investigation détaillée). Ce sont par exemple des pertes reliées à la baisse de satisfaction de la clientèle, le faible moral du personnel, la perte de confiance d'une partie de l'électorat à la suite d'un problème mettant en cause une entité gouvernementale ou la perte d'opportunités d'affaires pour une entreprise privée à la suite d'un risque qui s'est concrétisé. Dans certains cas, une tentative d'assignation d'une valeur monétaire pourra s'avérer possible en posant la question « Quel montant l'organisation serait- elle disposée à investir afin de corriger la situation résultant d'un risque qui s'est concrétisé ? » Par exemple, s'il s'agit d'une perte reliée à la baisse de satisfaction de la clientèle, une organisation pourra être disposée à investir un montant donné en publicité et en compensation afin de redorer son blason auprès de sa clientèle.

1.1.4 Bénéfices

Bien sûr, la gestion des risques comporte des coûts liés à l'intégration de nouvelles activités à la gestion de projet. Cependant, les bénéfices à en retirer compensent largement les coûts, tant sur le plan financier que sur les plans stratégique, politique, administratif et humain.

Il suffit de rappeler les résultats d'une étude récente effectuée aux États-Unis (Chaos, Standish Group, 2003)paru dans le «Standish Press release» du 25 mars 2003 :

- Le taux de succès des projets au augmenté juste un peu au-dessus du tier soit 34% pour l'ensemble des projets. Ceci représente une augmentation de 100% par rapport aux 16% de 1994.



- ➔ Les projets en échec, pour leur part, ont connu une diminution pour se rendre à 15% soit la moitié deu 31% de 1994.
- ➔ Les autres projets, avec dépassement de coût. Dépassement de calendrier ou diminutuion des fonctionnalités) obtiennent 51%.28 % des projets sont abandonnés en cours de développement ;

Le graphique sur La performance des projets informatiques parle de lui-même.

Bien que cette étude ait été faite aux États-Unis, il est raisonnable d'appliquer ces résultats aux projets réalisés au Québec. Quoiqu'il y ait eu une amélioration depuis 1994, il n'en demeure pas moins qu'une réduction des dérives des projets, ne fut-ce que de 10 %, représente des bénéfices importants.

De plus, bien souvent à des bénéfices élevés d'un projet correspondent des risques élevés et inversement, à des risques faibles correspondent des bénéfices faibles. Il est donc sain que des risques accompagnent les projets afin que l'organisation puisse en retirer des bénéfices appréciables. Cela accentue par contre encore plus l'importance de la gestion des risques dans les projets majeurs.

Au delà du bénéfice financier, d'autres bénéfices moins tangibles, mais tout aussi importants, peuvent découler de la gestion des risques. La gestion des risques permet d'obtenir un meilleur engagement et une meilleure communication de la part de tous les intervenants en rendant les risques plus explicites. Elle fournit aussi aux intervenants une possibilité de partage de leurs connaissances et de leurs expériences, ce qui les valorise d'autant. Enfin, la gestion des risques peut permettre de moduler les niveaux de contrôle des projets de la part des organismes centraux ; la marge de manœuvre accordée dans la gestion d'un projet ou même d'un portefeuille de projets pourra varier selon l'efficacité de la gestion des risques mise en place dans le ministère ou l'organisme.

La gestion des risques peut contribuer de façon significative à l'amélioration de la performance des ministères et organismes dans la gestion de leurs projets. Mais, comme le démontre le récent sondage, les gouvernements ne sont pas encore très outillés pour s'acquitter de cette tâche. Cela justifie encore plus l'importance de l'existence de ce site Web afin de soutenir les ministères et les organismes dans la gestion des risques et ainsi faire face aux enjeux des projets informatiques à venir.

1.2 Définitions

1.2.1 Historique de la gestion des risques

Le concept de gestion du risque ou Risk Management a fait son apparition aux États-Unis à la fin des années 1950. La dimension probabiliste d'une perte

financière et la question de l'assurance ont longtemps prédominé comme point de mire de la notion de risque.

Toutefois, au tournant des années 1980, l'étude du risque a étendu ses ramifications dans plusieurs champs d'activités, dont l'informatique. Au début, on utilisait des listes de contrôle pour identifier les facteurs de risque lors des études de faisabilité. Par la suite, les facteurs de risque ont été mis en relation avec les risques, i.e. les conséquences sur les délais, la qualité ou les coûts pour ne nommer que ceux-là. Aujourd'hui, il existe des outils intégrés d'analyse des risques ainsi qu'un certain nombre de modèles de gestion des risques adaptés à l'informatique. Celui du Software Engineering Institute – un centre de recherche et développement américain voué à l'amélioration des pratiques logiciel – retient l'attention de ce site Web.

En réalité, la gestion des risques a été longtemps appliquée de façon accessoire et implicite dans la gestion des projets informatiques. À l'heure actuelle, de plus en plus d'organisations formalisent un tel processus, surtout pour les projets d'envergure ou stratégiques. D'ailleurs, le « Project Management Institute »- un organisme international regroupant des professionnels en gestion de projets - définit la gestion des risques comme l'une des neuf pratiques clé de la gestion de projets. La gestion des risques connaît donc une popularité grandissante et fait maintenant partie des « meilleures pratiques » en informatique.

1.2.2 Risque

Le risque est un concept multidisciplinaire défini de plusieurs façons dans la littérature et au sein de l'industrie. Toutefois, un consensus se dégage à l'effet que le risque implique deux notions fondamentales : l'incertitude et une perte. Voici trois définitions :

- ➔ Le risque est une fonction, essentiellement le produit de la probabilité et de l'ampleur d'une perte.
- ➔ Le risque est la valeur potentielle d'une conséquence négative non désirée d'un événement ou d'une activité.
- ➔ Le risque est la somme des pertes multipliée par leurs probabilités.

Voici maintenant quelques **exemples de risques** (conséquences défavorables) caractérisant les projets informatiques :

- ➔ L'augmentation des coûts;
- ➔ La réduction des bénéfices;
- ➔ L'accroissement des délais;
- ➔ La perte de qualité du logiciel;
- ➔ La réduction de la fonctionnalité;

- ➔ La perte d'information;
- ➔ La perte de satisfaction du client.

1.2.3 Facteur de risque

Un facteur de risque est un élément déclencheur d'une perte, i.e. un événement ou une situation qui cause l'occurrence d'une perte. Le facteur de risque constitue donc l'origine d'un risque ou d'un ensemble de risques.

Parmi les exemples classiques de facteurs de risque, on retrouve la complexité d'une application, la taille d'un projet, le nombre d'intervenants, la nouveauté technique, l'instabilité des besoins d'affaire, le manque d'expérience, l'absence d'assurance qualité, le manque de rigueur dans la définition des exigences, de paramètres erronés d'estimation de l'effort, etc.

Dans la plupart des méthodes de gestion des risques, et parfois dans certaines organisations, on retrouve des listes exhaustives de contrôle des risques qui nous aident à identifier les facteurs de risque pouvant s'appliquer à un projet donné. Généralement, un sous-ensemble limité de ces facteurs caractérise les enjeux d'un projet.

1.2.4 Analyse du risque

L'analyse du risque est l'étude systématique des forces et des entités comportant un potentiel d'influence négative sur l'atteinte d'objectifs. Ainsi, l'analyse cherche à expliquer le phénomène du risque de façon à mieux en connaître les impacts et à mieux définir des avenues de solution.

Une analyse comporte généralement une mise en contexte, un énoncé mettant en relation le risque et les facteurs de risque, des caractéristiques du risque comme le niveau de contrôle, les conséquences indirectes, les individus ou groupes visés, etc. On retrouve des exemples d'analyses de risques dans la Banque de risques et dans la phase d'analyse de risque.

1.2.5 Gestion des risques

La gestion des risques est un processus comprenant des étapes bien définies et suivies qui favorisent une meilleure prise de décision tout en fournissant une meilleure information sur les risques et leurs impacts. La gestion des risques concerne aussi bien l'identification d'opportunités que l'évitement de pertes. Encore une fois, le modèle de gestion de risques proposé dans ce site est celui du Software Engineering Institute.

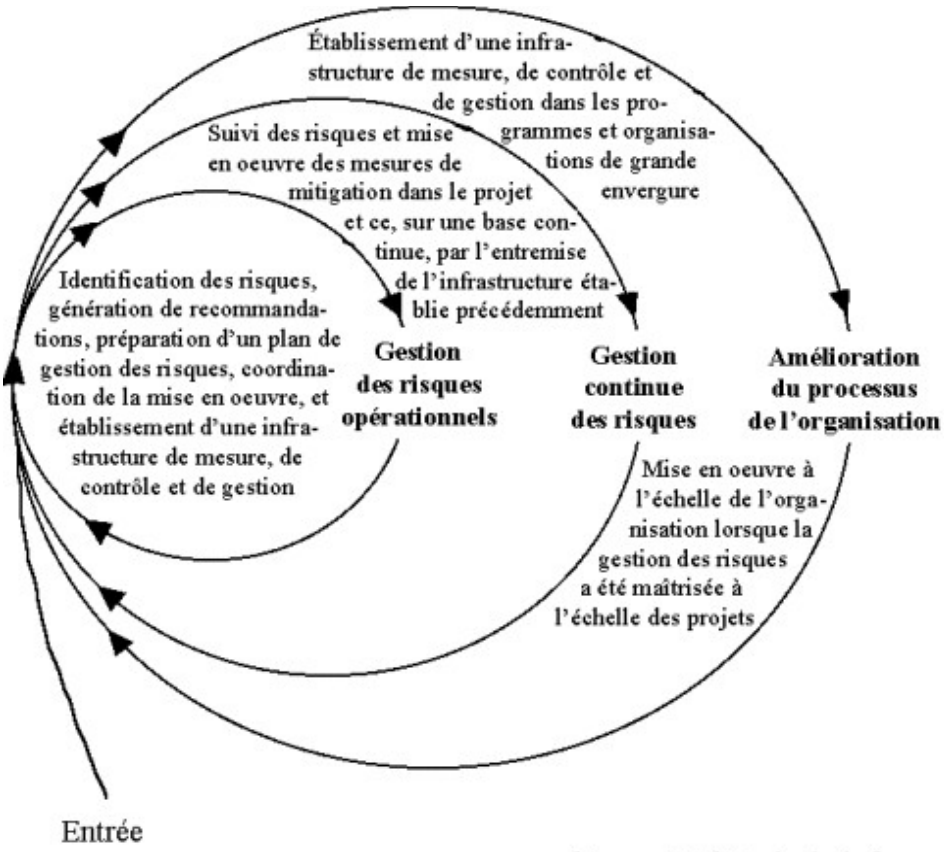
1.3 Concept de base sur la gestion du risque

1.3.1 Démarrage de la gestion du risque

Une démarche de gestion continue des risques requiert une infrastructure de gestion adéquate afin d'être réalisée d'une façon concluante. Autrement, la gestion continue des risques est susceptible d'alterner indéfiniment entre l'identification et l'analyse et éventuellement d'être abandonnée au fur et à mesure que le personnel arrive à la conclusion que celle-ci ne mène à aucune mise en œuvre effective de mesures de mitigation et de contingence.

Le diagramme suivant représente une approche de démarrage et d'implantation de la gestion des risques au sein d'une organisation. L'approche comprend trois phases distinctes et la stratégie sur laquelle elle s'appuie est cohérente avec celle sur laquelle repose le CMM. Avant de définir et d'implanter un processus à l'échelle de l'organisation, le processus de gestion et de réalisation doit en premier lieu être stabilisé dans chaque projet de développement d'applications. De même, les risques découlant de la façon d'intégrer les ressources humaines, les méthodes, les procédures, les outils et les équipements (ci-après désignés par risques opérationnels) au sein d'un projet doivent en premier lieu être maîtrisés avant d'être en mesure de gérer les risques de toute nature et de façon continue dans un projet. À plus forte raison, il est nécessaire de maîtriser la gestion des risques dans chaque projet avant d'être en mesure de les gérer au sein d'une organisation dans laquelle plusieurs projets sont simultanément en cours de réalisation.

Démarrage et évolution de la gestion des risques dans une organisation



[Source: GRafP Technologies]

Dans leur forme la plus simple, les trois phases sont mises en œuvre de façon séquentielle. La première phase (boucle interne du diagramme) consiste à établir l'infrastructure à l'échelle des projets dans le but de gérer les risques de nature opérationnelle avec lesquels ils doivent composer. L'objectif premier de cette phase est d'améliorer les chances d'une réalisation concluante des projets en question, en réduisant la fréquence ou l'impact des problèmes reliés à la façon dont les ressources humaines, les méthodes, les procédures, les outils et les équipements sont intégrés. À cet égard, l'approche de gestion des risques présentée plus loin peut être mise à contribution.

La démarche S:PRIME (Software: Process Risks Identification, Mapping and Evaluation) aborde principalement ce type de risques et fournit un soutien méthodologique et technique à l'identification, à l'analyse et à la planification de mesures de mitigation de ces risques. Une fois que cette infrastructure a été établie, une transition à la deuxième phase (boucle centrale du diagramme) peut être effectuée. Cette phase vise à gérer tous les risques auxquels les projets sont exposés (autant les risques opérationnels que les risques intimement reliés à un projet en particulier) et ce, sur une base continue.

Finalement, après qu'une gestion continue des risques a été maîtrisée au sein des projets, la troisième phase (boucle externe dans le diagramme) peut être entreprise. Celle-ci consiste essentiellement à mettre en œuvre une approche de gestion des risques à l'échelle de l'organisation et à augmenter la capacité de

cette dernière à réaliser les projets de développement et d'entretien d'applications qui y sont entrepris.

Suggestions pour le démarrage

- ➔ Commencez dès maintenant !
- ➔ Assignez la responsabilité de coordonner et de gérer les risques.
- ➔ Établissez des réserves en temps et en ressources pour la gestion des risques.
- ➔ Au début, appliquez une approche qualitative et au fur et à mesure qu'elle est appliquée et maîtrisée, introduisez des approches quantitatives.
- ➔ Formalisez le suivi et la revue des risques dans le cadre des revues de projet.
- ➔ Établissez un mécanisme de communication des risques et des problèmes résultant de ceux (prévus ou imprévus) qui se sont matérialisés.
- ➔ Établissez des groupes de soutien chargés de supporter les phases d'identification et d'analyse des risques, les phases de planification et de suivi des mesures de mitigation et de contingence et la phase de contrôle des risques.
- ➔ Faites la promotion d'échanges d'information à tous les niveaux hiérarchiques.
- ➔ Établissez et mettez à jour un répertoire des 10 risques les plus importants auxquels le projet est exposé.
- ➔ Définissez un processus de gestion de crises et assurez-vous qu'il est connu de tous les intervenants au projet.

Dans les projets de faible envergure :

- ➔ développez un script décrivant les étapes à réaliser afin de gérer les risques, quand elles doivent l'être, et par qui;
- ➔ utilisez des formulaires simplifiés pour l'identification des risques;
- ➔ identifiez les risques dans le cadre de réunions périodiques (p. ex. mensuelles) avec l'équipe de projet à l'aide d'une liste de contrôle préétablie;
- ➔ préparez des mesures de mitigation et de contingence sous la forme de listes de points d'action;
- ➔ réalisez les activités de gestion des risques de façon périodique plutôt que continue et à chaque phase de développement mais réalisez-les bien.

Facteurs de succès

Les facteurs contribuant le plus au succès de la gestion des risques dans un projet sont les suivants :

- ➔ le niveau de soutien qui y est accordé par le personnel de direction du projet;
- ➔ le degré de visibilité dont bénéficient les activités de gestion des risques et les résultats obtenus;
- ➔ l'adéquation des ressources budgétaires et humaines qui y sont allouées;
- ➔ la qualité du processus mis en œuvre à cette fin et son évolution en fonction des expériences vécues;
- ➔ la formation et la sensibilisation dispensées;
- ➔ la quantification des activités et des résultats obtenus.

1.3.2 Modèle des meilleures pratiques en gestion des risques du SEI

NOTE : Un modèle des meilleures pratiques visant à mettre en œuvre une gestion des risques a été développé par le Software Engineering Institute en collaboration avec l'industrie. Le modèle en question fait présentement l'objet d'une revue à l'échelle internationale et il est susceptible d'évoluer dans les prochains mois et au cours des années qui suivront son déploiement. Il estprésenté ci-après car le modèle CMM-I (Capability Maturity Model® –Integrated –Systems/Software Engineering) duquel il est extrait est susceptible de devenir une norme de facto dans l'industrie au cours des prochaines années, si l'on en juge par la large diffusion dont a fait l'objet le CMM.

La gestion des risques est un processus continu qui intègre à la fois les processus d'affaires et les processus de gestion technique. La gestion des risques doit aborder les questions qui pourraient mettre en péril des objectifs critiques.

Une gestion des risques efficace requiert une identification rapide et agressive des risques potentiels. Un fort leadership est nécessaire au sein de chacune des parties affectées afin d'établir un environnement propice aux discussions ouvertes au sujet des risques.

Même si les éléments techniques sont d'un intérêt capital à la fois au début et à chacune des phases du projet, la gestion des risques doit également considérer les sources internes et externes concernant les coûts, les échéanciers et les risques techniques. Une détection rapide et agressive des risques est avantageuse, parce qu'il est plus facile, moins coûteux et moins dommageable d'effectuer des modifications et d'apporter des corrections au travail en cours que d'effectuer des changements sur le produit ou sur des éléments du projet en plein milieu ou à la fin du processus de développement.

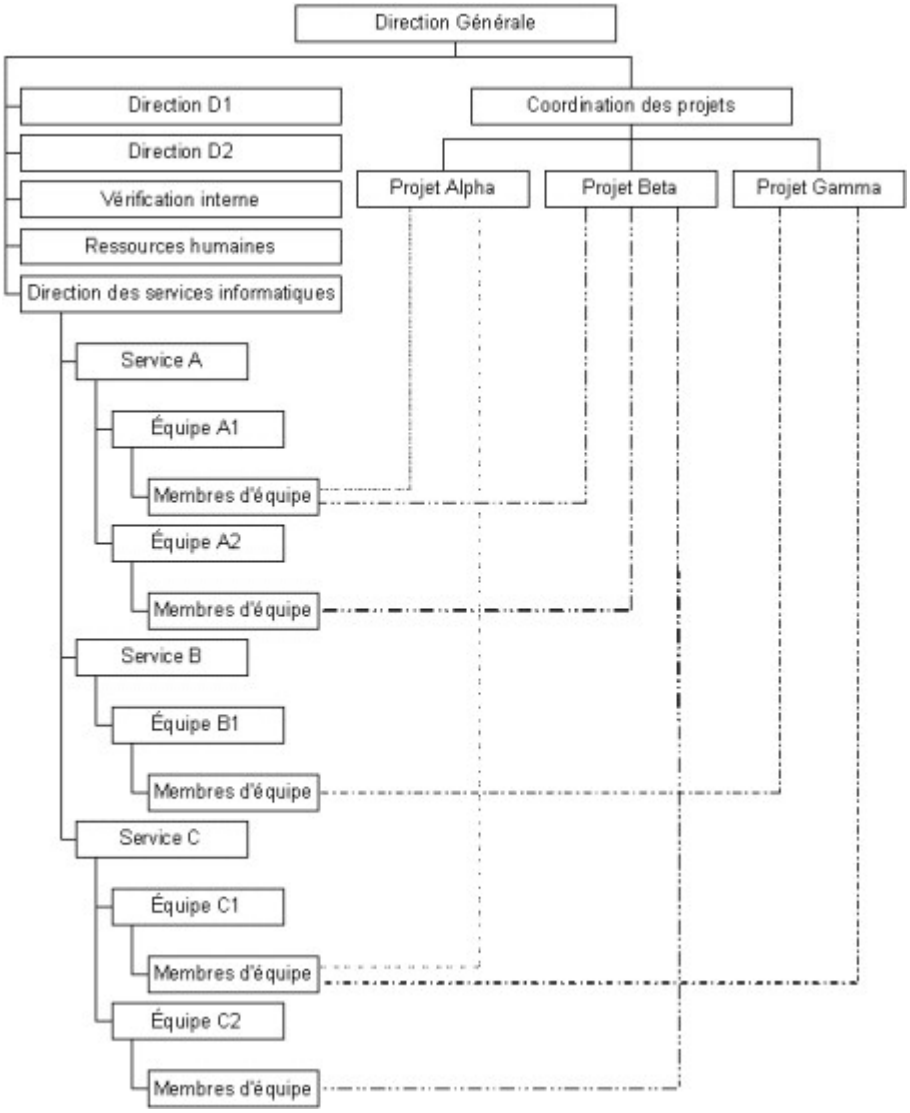
La gestion des risques peut être répartie en trois phases : la définition d'une stratégie de gestion, l'identification et l'analyse des risques, le développement de plans de réduction des risques mis en application lorsque nécessaire.

Consulter le modèle de pratiques en gestion des risques du SEI (430 Ko)

La structure organisationnelle à l'intérieur de laquelle s'intègre la gestion des risques varie évidemment d'une organisation à une autre. Le diagramme suivant présente une structure organisationnelle générique telle qu'elle est susceptible d'être rencontrée dans les organisations faisant appel aux technologies de l'information.

1.3.3 Structure organisationnelle générique

Lors de l'implantation d'une structure de gestion des risques, il est important de prendre en considération le fait que certaines fonctions contribuent à l'efficacité d'une gestion des risques à l'intérieur d'une organisation. Si la liste présentée ci-dessous peut sembler exhaustive, il faut cependant noter qu'au sein de petites ou moyennes organisations, une même personne peut occuper plusieurs de ces fonctions.



Promoteur du projet(ex. : direction générale, direction des services informatiques)

- ➔ Supervise et offre le soutien nécessaire à la gestion des risques
- ➔ Assure un lien étroit entre la gestion des risques et les objectifs de l'organisation
- ➔ Donne les pleins pouvoirs aux groupes chargés de la gestion des risques selon leur rôle respectif
- ➔ Supervise et offre le soutien nécessaire à l'implantation de la gestion des risques

Chef de projet

- ➔ Désigne les personnes assignées à la mise en œuvre de la gestion des risques et s'assure que leurs rôle et responsabilités sont clairement définis
- ➔ Désigne un responsable assigné au projet
- ➔ Assure des ressources et un financement adéquat pour la gestion des risques
- ➔ Supervise la progression de la gestion des risques

Chef de service

- ➔ Encourage le travail de gestion des risques à l'intérieur de son équipe de travail
- ➔ Évalue les performances de son équipe de travail et rapporte l'information relative au risque, s'il y a lieu

Chef d'équipe (agissant en tant que promoteur de la gestion des risques au sein du projet)

- ➔ Dirige les changements relatifs à la gestion des risques en cours de projet
- ➔ Supervise, incite et encourage la gestion des risques
- ➔ Établit un compte-rendu de la progression du travail destiné au chef de projet

Agent de changement(ex. : service des méthodes et outils)

- ➔ Développe et met à jour un standard organisationnel pour la gestion des risques (ex. : évalue les outils et les méthodologies existantes, émet des recommandations)
- ➔ Établit des lignes de conduite et des critères de conception dans le but d'adapter une gestion des risques organisationnelle aux besoins des projets
- ➔ Contribue à adapter le processus de gestion des risques aux besoins des projets, si nécessaire
- ➔ Développe et met à jour les outils de gestion des risques (ex. : base de données sur les risques rattachés au projet et sur les stratégies de mitigation des risques)
- ➔ Développe et met à jour les documents portant sur le processus de gestion des risques (échantillons de plans concernant la gestion des risques)
- ➔ Coordonne et participe à l'évaluation des risques dans les projets
- ➔ Travaille en collaboration avec le chef d'équipe agissant en tant que promoteur de la gestion des risques au sein du projet

Conseiller ou formateur(ex. : ressources humaines)

- ➔ Fournit les expertises concernant la gestion des risques

➔ Dirige les sessions de formation

Modérateur/Animateur (ex. : service des méthodes et outils, assurance qualité, vérification interne, etc.)

➔ Fournit le soutien pour l'adaptation des méthodes et des outils de travail

➔ Participe à la résolution de conflits

➔ Fait part des progrès au promoteur du projet, le cas échéant.

Personnel assigné au projet (ex. : membres d'équipe)

➔ Maintient une communication ouverte au sujet des risques

➔ Contribue à l'identification, à l'analyse, au suivi et au contrôle des risques, s'il y a lieu

2 Orientations gouvernementales

Un nouveau cadre de gestion des ressources informationnelles (R.I.) a été approuvé par le Secrétariat du Conseil du trésor (SCT) le 29 janvier 2002 et est entré en vigueur le 1er avril.

Ce nouveau cadre précise les buts à atteindre, identifie les rôles et responsabilités des intervenants et établit un ensemble de mécanismes de gouverne et de soutien qui, tout en responsabilisant les ministères et organismes, assurent le maintien de la cohérence gouvernementale en matière de ressources informationnelles instaure des mécanismes de coordination qui remplacent en majeure partie les autorisations préalables fondées sur des seuils financiers. Ainsi :

Les ministères et organismes sont appelés à soumettre annuellement au Conseil du trésor un plan de gestion des ressources informationnelles et un bilan de gestion de gestion des ressources informationnelles qui précisent notamment les projets, les coûts, les bénéfices, les risques et les résultats attendus et réalisés;

Dans le cadre de gestion des ressources informationnelles, on y stipule au paragraphe 5.2.1 « Ce plan de gestion des ressources informationnelles fait notamment le lien avec les objectifs stratégiques de l'organisation. Il détermine le portefeuille de projets de développement... évalue les risques et précise les résultats attendus. » Il n'est pas fait mention, pour la première année de la façon dont les risques doivent être évalués, ni la façon de rendre compte. Toutefois, l'information présente sur le présent site correspond aux attentes du SCT en matière de gestion des risques.

De plus, ceux qui n'auront pas soumis leur plan stratégique, ont à se plier à la directive de 1995 et ainsi souscrire au contenu du présent site. Voici les orientations gouvernementales correspondantes au contenu de la directive de 1995.

Le Conseil du trésor a décidé, en avril 1995, des modalités de gestion des projets majeurs au gouvernement du Québec. Parmi ces modalités, figurent les éléments de documentation de ces projets qui sont consignés dans le document intitulé

*Mémoire de présentation d'un projet de solution d'affaires impliquant un recours aux technologies de l'information (projet ministériel) (21 Ko). Ce document comprend les indications suivantes concernant la gestion des risques :

« 12.2 Gestion des risques (analyse du risque et propositions pour y pallier)

(Plan de gestion des risques) »

Fort de l'expérience de l'application de cette décision, le Secrétariat du Conseil du trésor (SCT) a considéré qu'il était important d'insister encore davantage sur la nécessité de gérer les risques dans les projets informatiques et, en conséquence, de donner les moyens aux ministères et organismes pour faciliter cette gestion des risques. À cet effet, il a mis en place un ensemble de mesures visant à mieux les soutenir dans cette gestion. Ces mesures sont de cinq ordres:

Précision des informations à fournir en matière de gestion des risques.

Le SCT a produit un document intitulé

*Éléments d'information à fournir sur l'analyse et le plan de gestion des risques pour un projet ayant recours aux technologies de l'information (9 Ko). Ce document permet d'identifier quelles informations sont attendues par le SCT afin de lui permettre d'effectuer l'analyse d'un projet. Afin d'illustrer une analyse et un plan de gestion des risques, un exemple de chacun d'entre eux est fourni dans le document intitulé

*Gestion des risques en développement d'applications -Exemples - analyse et plan de gestion des risques (26 Ko). Ce document présente un exemple; il ne se veut pas être un format obligé de documentation de l'analyse et de plan de gestion des risques. Cet exemple est fortement teinté de l'approche de gestion des risques privilégiée par le SCT.

Identification d'une approche privilégiée pour analyser et gérer les risques

Analyse des risques

Le SCT a examiné différentes approches possibles d'analyse des risques et a retenu, comme première approche, S:PRIME (Software: Process Risk Identification, Mapping and Evaluation) développée par le Centre de recherche informatique de Montréal (CRIM). Les principaux motifs qui ont justifié ce choix reposent sur :

- le fait que la méthode a recours à des modèles de référence reconnus et accessibles, soit le Modèle d'évolution des capacités (CMM) et la

- ➔ taxonomie des risques du Software Engineering Institute (SEI);
- ➔ la disponibilité de ressources compétentes au Québec pour effectuer ces analyses;
- ➔ la formalisation de l'approche *S:PRIME (229 Ko) de sorte qu'elle puisse être répétée;
- ➔ le fait que des données quantitatives sont disponibles sur l'interprétation des résultats.

Même si le SCT privilégie l'approche S:PRIME, il n'en fait pas une approche obligée. D'autres approches peuvent être utilisées. Cependant, le SCT demandera alors au ministère ou organisme la documentation sur les modèles de référence utilisés et la méthode d'analyse utilisés par cette autre approche. Il est attendu que celle-ci soit aussi bonne sinon meilleure que l'approche S:PRIME pour le projet ou le portefeuille de projets concerné. Éventuellement, cette autre approche pourra devenir une des approches privilégiées.

Gestion des risques

De la même façon, le SCT privilégie un processus de gestion des risques, cette fois- ci développé par le SEI. Ce processus jouit d'un large consensus, a fait l'objet de plusieurs publications et se retrouve sous une forme presque identique, dans la version 1999, à la norme australienne sur la gestion des risques

Risk management (AS/NZS 4360:1999) Ce processus est défini à la section Démarche du site.

Organisation de sessions de sensibilisation et de formation en gestion des risques.

Le SCT, en collaboration avec le CRIM et GRafP Technologies, peut organiser des sessions de sensibilisation et de formation en gestion des risques. Consulter la section Formation pour en savoir davantage.

Développement et soutien d'un site Web en gestion des risques.

Le SCT, en collaboration avec plusieurs partenaires, a développé ce site Web qui facilite l'accès aux connaissances en gestion des risques et incite au partage des connaissances entre les ministères et organismes.

Mise sur pied d'un groupe d'intérêt en gestion des risques.

Un groupe d'intérêt a été mis sur pied afin de faciliter encore davantage le partage de connaissances, de soutenir le site Web et de maintenir un échange continu entre le SCT et les ministères et organismes. Vous pouvez contacter le responsable du groupe à marc.laurin@sct.gouv.qc.ca.

3 Processus de gestion des risques

Le schéma présente les six phases de gestion des risques retenues dans ce site pour représenter le processus de gestion des risques.

Pour chacune des six phases, vous retrouverez : une présentation synthétique (Survol de la phase), une présentation détaillée (Détail de la phase), des témoignages, des gabarits, des conseils et des exemples.

En résumé, les six phases de la gestion des risques s'effectuent tour à tour tout au long d'un projet. Elles se lisent dans le sens des aiguilles d'une montre.

Ainsi, la phase d'IDENTIFICATION () est généralement celle qui initie la gestion des risques; elle est suivie par l'ANALYSE (), la PLANIFICATION (), le SUIVI () et le CONTRÔLE ().

La phase de COMMUNICATION () est une exception car elle ne suit pas d'ordre chronologique et s'applique àl'ensemble des phases de gestion des risques.

4 Autres références

4.1 Guides et modèles

Nom	Description
Capability Maturity Model Integration (CMM-I)	Modèle intégré d'évolution des capacités logiciel, matériel et produit selon une représentation par niveaux ou continue. La représentation par niveaux définit la gestion des risques comme un secteur de processus à part entière au niveau de maturité 3 tout en conservant une préoccupation d'activités minimales en gestion des risques intégrées à d'autres secteurs de processus de niveau de maturité 2.
Capability Maturity Model Integrated (CMMI) - Risk management()	Modèle de pratiques du secteur de processus « Gestion des risques » du niveau 3. Traduction française de la version originale anglaise CMMI v1.1 publiée le 11 janvier 2002, représentation par niveaux.

Nom	Description
Continuous Risk Management Guidebook	Guide de gestion des risques en génie logiciel. Décrit une démarche complète du processus de gestion des risque. S'apparente au modèle présenté dans ce site Web.
Introduction to Team Risk Management	Guide de gestion des risques en équipe appliquée au génie logiciel. Favorise notamment la participation des clients et des fournisseurs dans les différentes étapes de gestion des risques.
Project Management Body of Knowledge (PMBOK)( )	Guide de gestion de projet du « Project Management Institute » incluant un volet en gestion des risques. Sert de référence à la certification des professionnels en gestion de projet.
Project Zeus Risk Management Plan at NASA	Modèle et exemple de gestion des risques pour le projet Zeus à la NASA.
Software Acquisition Risk Management Key Process Area-A Guidebook	Guide de gestion des risques appliquée à l'acquisition de logiciels. Décrit toutes les étapes ainsi que les critères pouvant être utilisés pour procéder à une sélection juste et efficace.
Software Development Risk: Opportunity, Not problem.	Guide d'introduction au concept de la gestion des risques en informatique. Présente une perspective sur le contexte et les enjeux
Taxonomy Based Risk Identification	Guide de gestion des risques en informatique proposant une classification exhaustive des risques.
S:PRIME	Méthode d'évaluation des risques en développement et entretien d'applications informatiques s'appuyant à la fois sur le CMM et sur la taxonomie des risques mis au point au Software Engineering Institute

4.2 Logiciels

Nom	Description
@RISK	Outil d'analyse du risque sur Excel qui utilise la simulation Monte-Carlo
@RISK for Project	Outil d'analyse du risque sur Microsoft Projet qui utilise la simulation Monte-Carlo.
Crystal Ball	Outil d'analyse du risque et de projection qui utilise la simulation Monte-Carlo.
DATA	Outil d'analyse décisionnelle en contexte d'incertitude
DSE Manager	Outil d'analyse du risque en informatique
IEEE- SERIM	Outil de gestion des risques en génie logiciel développé et supporté par l'IEEE. Permet d'évaluer 3 types de risques - coûts, délais et techniques - à partir de l'évaluation d'une série de facteurs de risque
Microsoft IT Advisor for Risk Management	Outil d'évaluation des risques dans différents contextes de projets informatiques basé sur une évaluation des probabilités et de l'impact d'une série de facteurs de risque.
RightWare	Outil de conseil et d'analyse du risque en informatique
Risk Driver	Outil d'analyse financière du risque
Risk Master	Outil d'analyse du risque de plan de projet qui utilise la simulation Monte-Carlo
Risk Radar	Outil de gestion des risques sur Excel
Riskman	Outil de gestion du risque en général soutenu par une base de données.
S:PRIMER	Outil d'évaluation du niveau de risque d'un projet informatique basé sur la taxonomie des risques et le modèle d'évolution des capacités (CMM) du Software Engineering Institute.

4.3 Personnes-ressources

Personnes-ressources internes aux ministères et organismes

Nom	Organisme ou ministère	Coordonnées

Jean Veilleux	Régie des rentes du Québec	Jean.Veilleux@rrq.gouv.qc.ca Tél.: (418) 657-8725 poste: 3504
Luc Vincent	Conseil du trésor - SCT	luc.vincent@sct.gouv.qc.ca Téléphone : (418) 528-9746

4.4 Centres d'intérêt et instituts

Nom	**Description**
Cirano	Centre inter universitaire de recherche en analyse des organisations. Comporte un volet sur la gestion intégrée des risques et un autre sur les risques technologiques majeurs.
CRIM	Centre de recherche informatique de Montréal œuvrant notamment en gestion des risques.
Decision Analysis Society	Site de référence universitaire sur la décision et l'analyse du risque chapeauté par la Duke University.
Decision Science Institute	Site de référence universitaire sur la décision et l'analyse du risque chapeauté par le Georgia State University. Orienté publications et recherches. Publie le Decision Science Journal.
KPMG	Firme comptable qui réalise annuellement un sondage sur la gestion des risques en général au Canada.
Program & Project Risk Management @Ames Research Center	Site pédagogique sur la gestion des risques soutenu par la NASA.
Risk Management of Australia	Site de référence sur la gestion des risques du groupe de normalisation australien, le Standard Australia Group. On y retrouve un modèle de gestion des risques.
RiskWorld	Site multidisciplinaire et indépendant sur la gestion et l'analyse des risques. Fournit une vision élargie du risque dans divers aspects de la société et de l'économie.

Nom	Description
The Standish Group International	Groupe de recherche sur les logiciels critiques et sur le commerce électronique. A publié deux rapports importants sur l'état de l'industrie en gestion des risques : « Chaos » et « Unfinished Voyages ».

4.5 Normes

Le guide CAN/CSA-Q850 vise à aider les décideurs à gérer efficacement les différents types de risques, notamment les risques de blessure et de danger pour la santé, les biens, l'environnement et toute autre valeur. Ce guide explique le processus d'acquisition, d'analyse, d'évaluation et de communication de l'information nécessaire à la prise de décision.
La présente section de la CEI fournit des lignes directrices permettant de choisir et de mettre en œuvre des techniques d'analyse du risque, principalement pour l'évaluation du risque de systèmes technologiques. L'objectif de la présente norme est d'assurer la qualité et la cohérence de planification et d'exécution d'analyse des risques, ainsi que de présenter les résultats et les conclusions correspondants.
Cette norme constitue un guide pour l'élaboration et la mise en oeuvre d'un processus de gestion des risques incluant : l'identification, l'analyse, l'évaluation, la mitigation (treatment) et le suivi des risques

5 Gabarits, guides et exemples

Certains gabarits peuvent être téléchargés en format Word (Word), d'autres en format PDF () (avec le logiciel Acrobat Reader).

Cliquez sur le symbole correspondant.

Si vous n'avez pas le logiciel Acrobat Reader, téléchargez-le.

Gabarits

Fiche de risque.....Word (124 Ko)

Contient les sections « Identification », « Analyse », « Planification et suivi » et « Contrôle » des risques

Exemples

Exemple d'identification des risques	(11 Ko)
Exemple d'analyse	(14 Ko)
Exemple de planification et de suivi des risques	(23 Ko)
Exemple de contrôle des risques	(21 Ko)
Liste de contrôle pour l'identification des risques	(150 Ko)

6 Questions

Qui doit gérer les risques dans un projet informatique ?

Réponse : En fait, tous et chacun gèrent directement ou indirectement des risques d'une façon plus ou moins formelle. Les risques inhérents à la stratégie de projet sont généralement gérés par les dirigeants, les risques reliés à la gestion par le responsable de projet et les risques inhérents aux aspects techniques par les spécialistes et les informaticiens.

Dans certains cas, on peut déléguer la tâche à un individu, notamment dans les projets d'envergure et les projets stratégiques. Ce dernier s'assure que les risques sont bien identifiés, suivis et contrôlés par l'ensemble des intervenants d'un projet. Il joue donc un rôle de conseil et de coordination.

Dans d'autres cas, on peut faire participer les clients ou même les fournisseurs. Toutefois, l'individu ou le groupe responsable de livrer des solutions informatiques demeure toujours celui qui, en bout de ligne, est responsable des enjeux d'un projet, et par conséquent des risques.

Qu'arrive-t-il si on ne gère pas les risques d'un projet ?

Réponse : D'abord, la gestion des risques est forcément réalisée dans tous les projets. Cet exercice est toujours effectué, au moins intuitivement, mais de plus en plus, on lui accorde de l'importance et on lui associe des activités distinctes et des biens livrables déterminés.

Dans le cas des projets où on gère les risques de façon intuitive, ou au sein desquels on leur accorde peu d'importance, ces projets sont plus susceptibles de rencontrer des difficultés et d'aboutir à des situations pour lesquelles des solutions de rechange n'ont pas été prévues. De plus, il est beaucoup moins probable que les objectifs de délais, de qualité et de bénéfices soient atteints.

7 Formation

Sessions de sensibilisation à la gestion des risques

- ➔ Pourquoi gérer les risques lors des projets de développement d'applications ?
- ➔ Quelles en sont les grandes étapes ?

Une session de sensibilisation a été préparée afin de répondre à ces questions.

Cette session vise à :

- ➔ Sensibiliser les participants à la valeur et à la nécessité de la gestion des risques;
- ➔ Situer la gestion des risques en développement d'applications;
- ➔ Survoler les phases de la gestion des risques;
- ➔ Comprendre les grandes étapes de la méthode d'évaluation des risques S:PRIME (Software : Process and Risk Identification, Mapping and Evaluation).

Cette session de sensibilisation est organisée par le Secrétariat du Conseil du trésor selon la demande des ministères et organismes lorsque le nombre le justifie.

Pour toute demande de session, veuillez vous adresser à

luc.vincent@sct.gouv.qc.ca

ou

Patrice Di Marcantonio@msg.gouv.qc.ca