Evaluation des risques projet

Fabien Cleuet - CISA

Administrateur de l'AFAI

DIATHESE © 11/2001

L'an 2000 et l'euro sont des projets qui ont en commun d'imposer une maintenance lourde sur l'ensemble du système d'information. On peut d'ailleurs se demander quand les consultants auront de nouveau l'opportunité de côtoyer des projets transversaux aussi passionnants.

Certes, l'an 2000 était un sujet fondamentalement technique alors que l'euro présente une réelle dimension fonctionnelle et liée aux « métiers ». Dans les deux cas de figure, l'empleur du projet a imposé des équipes de pilotage importantes. Une de leurs activités consiste à évaluer le risque par sous domaine (ou application). La démarche présentée ci-après est un retour d'expérience issu d'un projet euro dans une banque.

1. RISQUES PROJET

Pour un projet aussi vaste que l'euro, l'évaluation du risque est une démarche visant à répondre aux questions suivantes :

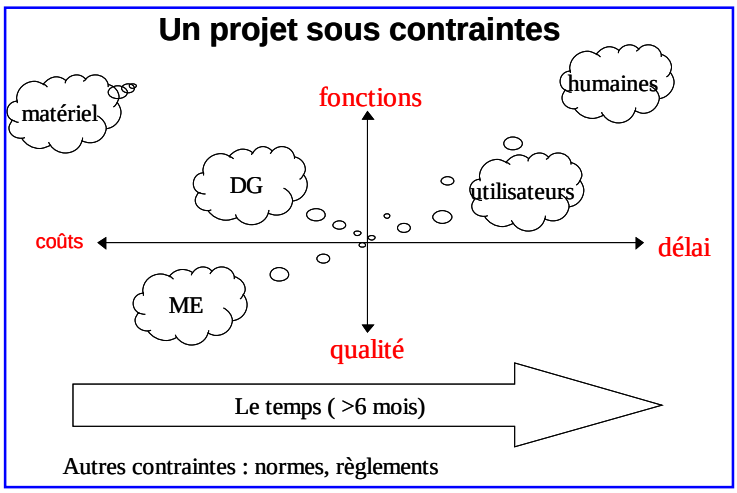
- quelles sont les applications ou domaines du projet dont l'enjeu stratégique ou financier est significatif ?
- quel niveau et quelle nature de risque ? (client, organisationnel, fonctionnel ou technique)
- quel plan d'action pour « traiter » ce risque ?
- quelle est la contribution des plans d'action pour maîtriser le risque ?

1.1 Une démarche pour plusieurs publics

Dans le cas d'un projet important, l'ensemble des acteurs de l'entreprise ont besoin d'indicateurs pour identifier, évaluer et suivre le niveau de risque de chaque sous partie du projet.

Destinataires	Préoccupations
La Direction Générale	Elle a besoin de connaître le niveau global du risque et enfin les plans d'actions pour le maîtriser.
La Direction des Systèmes d'information	C'est pour elle un outil de pilotage au même titre que le budget et le planning.
Les autres équipes projets	Il leur est nécessaire d'apprécier et de suivre le risque de leur propre projet mais aussi celui des projets ayant un impact technique ou organisationnel avec le leur.
L 'audit interne et l'auditeur externe	L'auditeur doit avoir une bonne perception du fonctionnement et de l'évolution du SI. Dans le cas présent, cette analyse du risque permet d'orienter les missions sur les « zones sensibles » en terme de métier, d'image de marque ou encore de système d'information.
Les utilisateurs	En tant que maître d'ouvrage, il est primordial de connaître le risque de leur projet et de disposer d'un moyen de mesure pour suivre son évolution.

2. POURQUOI UN PILOTAGE PAR LES RISQUES ?



Classiquement, le pilotage des projets est assuré notamment par les outils de planification que sont le budget et le planning. Pourtant, il est plus rare de trouver un outil mesurant le risque et surtout son évolution durant le déroulement d'un projet.

Cette situation est assez étonnante car tout projet est une optimisation sous la contrainte des quatre facteurs présentés dans le schéma ci-contre. L'expérience montre que toute action sur un axe impose un « rééquilibrage » sur un autre. Ainsi, l'ajout de fonctions suppose une augmentation des coûts, à défaut, c'est sur la qualité que l'on procèdera à un ajustement en allégeant notamment la documentation et les tests.

Observons maintenant la relation Utilisateur / DSI durant le projet. Si au démarrage, le « contrat » a bien été défini en fonction des quatre axes, l'attention de l'utilisateur sera progressivement focalisée sur les axes coûts, délai et fonctions. Cette propension sera de plus en plus forte vers la fin du projet. En pratique, cette érosion au fil du temps des critères de sécurité et de qualité va privilégier les objectifs opérationnels au détriment de la solidité du projet.

A l'évidence, le contexte change lorsque les échéances se rapprochent. L'optimisme et la concorde d'origine sont alors loin quand le budget devient rouge et que les difficultés techniques subsistent.

C'est dans ce contexte de projet long et complexe que l'utilisation systématique d'une démarche de scoring [1]du risque contribue à tout un ensemble d'actions structurantes pour la maîtrise du système d'information.

Si une cartographie du système d'information a été réalisée, cette démarche a conduit à stocker dans une base de données les caractéristiques des composants et des flux du système d'information. Cette base de données peut alors être enrichie ou mise à jour des informations recueillies lors de la démarche de scoring du risque.

Pour l'équipe de pilotage de projet, cet outil permet d'aller à l'essentiel en ciblant les lots ou systèmes devant être suivis de près et nécessitant donc un plan d'action.

3. OBJECTIFS DE LA METHODE

Ce document propose une démarche qui répond à un objectif d'évaluation globale et rapide par un scoring du risque propre à chaque module ou sous projet.

Les caractéristiques de cette méthode sont les suivantes :

- utiliser un ensemble d'axes d'analyse dont certains évaluent les enjeux du projet et d'autres les risques à proprement parler.
- mesurer chaque axe par un nombre de questions allant de 4 à 15.
- préparer des critères de cotation objectifs pour toutes les questions, ce point fait l'objet d'un approfondissement ci-après.
- collecter l'information lors d'entretiens avec les personnes concernées en les conduisant à s'auto évaluer.
- procéder à une évaluation croisée de la maîtrise d'ouvrage (MOA) et de la maîtrise d'œuvre (MOE). Ainsi, les questions concernant la MOA seront aussi posées à la MOE afin de recueillir leur opinion et de s'assurer de la cohérence des évaluations de chaque partie. On procède réciproquement pour les questions concernant la MOE.

4. CRITERES DE COTATION

Cotation	Signification
0	Aucun risque
1	Risque dont l'impact est mineur
2	Risque dont l'impact est significatif mais maîtrisable
3	Impact grave et pénalisant pour l'activité de la société

[1] Le scoring est une mesure du risque selon une échelle de valeur.

5. SCORING

Le travail préalable d'identification des axes d'analyse et des critères de cotation est déterminant. Il doit donc être stabilisé avant le début des évaluations. Cette méthode a été mise au point dans le cadre d'un projet euro en utilisant les quatre axes suivants :

Axes	Thèmes évalués
Enjeu euro (A1)	• Poids financier de la maintenance • Stade d'avancement de l'application depuis la pré-étude jusqu'aux tests • Date de mise en œuvre ; plus celle-ci est proche du 31/12/01 plus on augmente le risque systémique
Enjeu stratégique et financier (A2)	• Contribution éventuelle de l'application au CA • Impact d'image interne externe et institutionnelle • Utilité de l'application (système : client, métier, interne, communication, …)
Risque Maîtrise d'ouvrage (A3)	• Expérience du Chef de projet utilisateur en matière d'analyse et d'expression des besoins • Difficultés d'organisation ou pénurie de ressources pour contribuer au projet • Stabilité des besoins métiers
Risque Maîtrise d'œuvre (A4)	• Maîtrise technique des traitements • Maîtrise technique des outils associés • Connaissance du fonctionnel par la MOE • Fréquence et difficulté de la maintenance • Qualité documentaire • Nombre et complexité des interfaces • Interconnexion avec d'autres systèmes • Disponibilité d'environnement de test • Difficulté des migration de données

5.1 Comment ajuster le périmètre de l'étude ?

- Il faut adapter vos questionnaires en sachant que sur les axes MOA et MOE il suffit le plus souvent d'une dizaine de questions pour faire le tour du sujet et cerner le risque. Au delà, les entretiens sont plus longs et ceux qui y participent peuvent éluder le problème par des réponses peu précises.

- Il importe enfin de tenir compte des risques propres à l'organisation et au métier exercé.

5.2 Comment objectiver les critères de scoring de chaque question ?

Attribuer une cotation (ou une note) est un exercice délicat dès lors qu'il est fait de manière rigoureuse.

Dans le cas des questions objectives basées sur des informations disponibles (date, chiffre d'affaire, coût, nombre de programmes,…) il ne s'agit que d'étalonner la cotation en fonction des valeurs maximales et minimales de la population.

Les questions subjectives sont par nature moins simple à normer. Il en est ainsi de la capacité des individus, de la qualité et la conformité documentaire ou encore de la maintenabilité[2] d'une application.

Cet exercice mérite une sérieuse réflexion. Il est judicieux de suivre les étapes suivantes pour déterminer les critères de cotation des questions subjectives:

1. La première étape consiste à vérifier l'existence d'un reporting sur ce sujet ou abordant ce sujet. Dans l'affirmative, on valide l'exhaustivité et l'actualité de ce reporting. Une fois ces critères satisfaits, on ne peut que privilégier l'utilisation de ces informations dont la qualité est reconnue.
2. Les processus de l'entreprise intègrent éventuellement des critères de qualité : norme d'architecture applicative, norme de documentation ou encore d'une journalisation événementielle telle celle des incidents d'exploitation. Ainsi, l'existence d'un référentiel ou l'analyse du passé peuvent constituer des éléments objectifs de cotation.
3. En l'absence de toute information ou système de mesure pré-existant, il faut créer ses propres critères en privilégiant la prudence et l'ouverture. La prudence signifie ici qu'il ne faut pas fixer les seuils de qualité trop bas. L'ouverture suppose que ces critères soit éventuellement discutés avec des interlocuteurs incontournables : RSSI[3], responsable étude, responsable méthode, chef de projet, ….

Dans tous les cas de figure, les critères doivent être stabilisés dès que possible et avant toute publication de résultat.

Enfin, le critère d'évaluation ne doit pas reposer sur une investigation poussée (évaluation de la documentation par exemple) car cela conduirait à renoncer à deux caractéristiques essentielles mentionnées ci-dessus : la rapidité de mise en œuvre et l'auto-évaluation.

5.3 Comment mesurer le risque ?

- Au cours des entretiens chaque question fait l'objet d'une cotation (cf §4) de 0 à 3

---

[2] Par ce terme, on mesure la possibilité de maintenir une application et par ailleurs, la difficulté des actions de maintenance passées.

[3] Responsable de la Sécurité du Système d'Information

- Pour chaque axe, nous calculons une moyenne des scores qui ne tient pas compte des risques nuls. En effet, l'absence de risque sur un point donné (cotation 0) ne constitue pas une diminution du risque global.
- On détermine ensuite un indice de risque par application ou domaine qui résulte d'une moyenne pondérée des quatre axes. Après différentes simulations, la pondération suivante a été retenue : {A1+(3 X A2) + A3 + A4} / 6.
- L'objectif de cet indice est de mettre en évidence le risque inhérent aux applications significatives pour l'entreprise.

6. ENTRETIENS

Les entretiens sont réalisés avec les chefs de projet utilisateur (maîtrise d'ouvrage) et la DSI (maîtrise d'œuvre) afin de « croiser » les opinions de chaque partie. Lorsque l'évaluation est trop discordante, il convient de diversifier les sources d'information pour ensuite fixer prudemment la cotation des questions concernées.

L'application de cette démarche a permis de constater le peu de points de divergence entre MOA et MOE. Face à un professionnel neutre car externe, un chef de projet MOE sait reconnaître, en règle générale, que son application n'est que partiellement maîtrisée ou documentée. De même, un utilisateur lucide admet sans difficulté son peu d'expérience en démarche de test. Ces entretiens sont donc le début d'un recensement relativement objectif et exhaustif des actions à entreprendre.

Pour toute information significative ou si l'interlocuteur ne semble pas fiable, il demeure malgré tout nécessaire de valider les informations échangées lors de ces entretiens.

Les résultats de ces entretiens sont regroupés sur deux documents :

- scoring sur tableau suivi sur tableur
- plan d'action par application

7. PRODUIT FINI

Cette approche permet de restituer une information selon 4 axes :

- Deux indicateurs indépendants mesurent :
  - l'enjeu lié à l'évènement spécifique ayant déclenché l'étude, ici l'euro
  - l'enjeu stratégique et financier
- Deux indices déterminent :
  - le risque lié à la MOA,
  - le risque technique lié à la MOE

Ces éléments sont repris dans un tableau de synthèse à raison d'une ligne par application avec le scores des quatre axes plus un indicateur de risque. Ce dernier est calculé par la moyenne de chaque axe après pondération de l'indice stratégique et financier.

			enjeux		risques			Actions		
application	domaine	Chef projet	euro	strat / fi	MOE	MOA	Global	test	contournement	bascule
A	Clientèle	xxxxx	1.7	2.7	2.2	1.7	2.3	a faire	a faire	a faire
B	paiements	yyyyy	3.0	2.0	1.7	2.5	2.2	a faire	a faire	a faire
C	Gest. Risque	zzzzz	2.0	1.5	1.3	2.7	1.8	a faire	a faire	a faire
D	Clientèle	ttttt	2.0	3.0	1.1	1.8	2.3	a faire	a faire	a faire

Un tableau détaillé de ce type permet ensuite de constituer différentes analyses :

- par domaine métier
- par chef de projet

7.1 Tableau de synthèse par domaine applicatif ou chef de projet

Domaine métier	Strat & fi	Euro	MOE	MOA	Indice
Achats et stock MP	2.4	1.7	1.5	1.8	2.0
Gestion de production	1.1	2.1	1.8	2.1	1.6
Ventes facturation	2.5	2.0	1.8	1.4	2.2
Stock PF	1.5	1.8	1.1	2.1	1.6
Base clients	2.4	1.7	1.8	2.2	2.1
Comptabilité	2.5	2.4	1.9	1.8	2.3
Site Web	0.9	1.5	1.7	2.5	1.4
Infocentre	1.0	2.0	1.0	1.0	1.2
Total	1.9	1.8	1.7	2.0	1.9

8. ANALYSE DYNAMIQUE

Pour que ce travail apporte toute sa valeur ajoutée à l'entreprise, il convient de réunir deux conditions :

- Connecter directement cette démarche avec les plans d'action visant à limiter le risque. L'étude ne sera plus seulement passive en mesurant le risque mais active en y apportant des réponses.
- Actualiser régulièrement cette étude afin de mesurer et d'analyser l'évolution du risque par nature et par domaine applicatif.

Domaine métier	T1	T2	T3	T4
Achats et stock MP	2.0	2.0	2.0	2.0
Gestion de production	1.6	1.9	1.9	1.9
Ventes facturation	2.2	2.2	2.2	2.2
Stock PF	1.6	1.7	1.8	1.8
Base clients	2.1	1.4	1.3	1.1
Comptabilité	2.3	1.0	1.0	1.0
Site Web	1.4	1.8	1.9	1.9
Infocentre	1.2	1.3	1.2	1.0
Total	1.9	1.6	1.6	1.6

le tableau ci-joint propose un suivi de l'évolution du risque global actualisé à chaque fin de trimestre.

Un même travail d'analyse dynamique peut être fait par nature de risque MOA / MOE

Ce suivi est particulièrement intéressant puisqu'il permet de mesurer l'efficacité des plans d'actions mis en œuvre.

9. CONCLUSION

A l'évidence, une telle démarche de mesure du risque apporte beaucoup au pilotage des projets importants. Ce dernier est traditionnellement assuré par le budget et le planning, sans que le critère de qualité révélateur de risque ne soit toujours intégré avec la même priorité. La démarche qualité étant maintenant une préoccupation des entreprises, la gestion de projet informatique ne doit évaluer tout risque significatif susceptible de compromettre le succès du dit projet.

Pour toute remarque ou commentaire relatif à cet article veuillez contacter : fcleuet@diathese.fr