

Mener un audit externe efficace : les apports de CobIT

Pourquoi un audit externe ?

Les demandes d'audit portent principalement sur des structures, des programmes ou des projets. Selon le cas, les questions posées diffèrent, avec des recouvrements significatifs.

Dans le cas d'un audit de structure, le commanditaire demande d'abord une analyse des services qu'elle rend à des clients internes ou externes, avec une appréciation d'une part sur le périmètre (le « catalogue »), d'autre part sur la qualité de service, mesurée ou perçue. Il souhaite ensuite vérifier comment l'organisation mise en place utilise les moyens et régule les coopérations de la structure étudiée au sein de l'entreprise concernée et avec ses fournisseurs. De façon plus spécifique, la demande inclut parfois une analyse du traitement des projets prioritaires au sein de la structure.

Pour un audit d'un grand projet, la focalisation change radicalement et l'audit se concentre sur l'alignement du projet avec la stratégie de l'entreprise, le pilotage, la maîtrise du budget et du calendrier, la qualité technique de la solution, la conduite du changement.

L'audit d'un grand programme combine les deux types de demandes

précédentes : le programme coordonne plusieurs projets sur une assez longue durée. Il a donc une structure pérenne dont l'objectif majeur est de livrer progressivement les sous-ensembles fournis par les projets, en assurant leur coordination technique et leur synchronisation.

Les contraintes qui s'imposent à l'auditeur externe sont néanmoins similaires entre les différents cas. En premier lieu, le délai est toujours très réduit, de l'ordre de quelques semaines sur des périmètres parfois très complexes, avec un grand nombre d'acteurs. En effet, l'audit est souvent motivé par une situation de difficulté où les décisions ne peuvent être repoussées trop longtemps. Même pour un audit préventif (voir l'encadré « *Audit externe du programme Copernic au Ministère de l'Économie, des Finances et de l'Industrie* »), le commanditaire souhaite que la perturbation qu'il introduit soit d'une durée limitée. L'auditeur se doit d'étayer ses constats sur une convergence de pièces et de témoignages, mais il lui est demandé de collecter ces éléments en perturbant au minimum l'objet d'étude ! Une autre exigence porte sur l'exhaustivité. Même si les questions posées sont assez précises, l'auditeur ne peut ignorer



Bernard Mazoyer,
Directeur Général, Fontaine Consultants

des thèmes au risque de laisser dans l'ombre des facteurs de risque grave. Le commanditaire recherche enfin une indépendance totale de l'audit par rapport aux acteurs de la structure, du programme ou du projet examiné.

Ces variantes et ces contraintes s'appliquent à un service d'audit interne comme à une équipe externe. L'appel à un audit externe, alors qu'il existe un service interne, s'explique souvent par la recherche d'une combinaison spécifique de compétences, qui sont nécessaires pour aborder les différentes facettes du sujet : la compréhension du métier doit s'allier à la maîtrise des enjeux d'organisation, de conduite de projet, d'architecture informatique, de transformation. La demande est d'ailleurs parfois de conduire une démarche de coopération entre les auditeurs internes et externes.

Une démarche préventive

Copernic vise à mettre en place le compte fiscal, grâce auquel chaque contribuable aura une vision de l'ensemble de sa situation fiscale : pour un particulier, l'impôt sur le revenu, la taxe d'habitation, l'ISF, etc., avec l'état des paiements effectués pour chacun et des échéances à venir ; pour une entreprise, l'impôt sur les sociétés, la TVA, etc. Le contribuable pourra ainsi consulter et saisir les pièces de son dossier via de nombreux canaux (guichet, téléphone, Internet, etc.). Pour le Système d'Information de l'administration fiscale, c'est une transformation profonde, puisque ces différents impôts sont aujourd'hui gérés par des applications différentes, utilisées par des services différents, avec une séparation des rôles et des informations entre la taxation (quel est le montant de l'impôt ?) et le recouvrement (quand et comment le règlement est-il effectué ?).

Audit externe du programme Copernic au Ministère de l'Économie, des Finances et de l'Industrie.

Le compte fiscal



Le programme Copernic est un investissement considérable, de plus de 900 millions d'euros. Il se décompose en une trentaine de projets principaux qui sont livrés progressivement, depuis 2001 et jusqu'en 2009. Environ un millier de personnes contribuent directement à ce programme. Les méthodes de gestion et de coordination sont très formalisées, à hauteur de la complexité des travaux.

C'est dans ce vaste périmètre que les Directeurs Généraux (Direction Générale des Impôts et Trésor Public) ont souhaité, par un audit externe, obtenir une évaluation indépendante de la bonne utilisation des investissements qui sont engagés. L'audit demandé n'est donc pas une réponse dans l'urgence à des difficultés particulières, mais une démarche préventive, pour l'identification des risques et leur élimination.

Les axes d'audit

Fontaine Consultants a été retenu en 2004 pour effectuer une analyse à deux niveaux :

- le premier est global au programme, il porte sur la gouvernance d'ensemble, les relations entre projets, les contributions des entités transverses ;
- le second, plus focalisé, porte sur quelques projets complexes et critiques.

A chaque niveau, le cahier des charges stipulait une évaluation selon quatre axes :

- la cohérence du programme avec les choix stratégiques de la Direction Générale des Impôts et de la Direction Générale de la Comptabilité Publique ;
- la qualité des différents " référents documentaires " ;
- l'organisation et le pilotage du programme ;
- la synchronisation des chantiers du programme et des projets.

Après les travaux de 2004, la démarche mise en place prévoit un point de situation annuel en 2005, puis en 2006. Lors de ces points de situation, les auditeurs auront à analyser l'évolution du programme d'une année sur l'autre et à se pencher sur les projets en cours à ces dates.

La vue large

Face aux exigences, contradictoires, de délai et d'exhaustivité, le premier enjeu pour l'auditeur externe est de bien situer les acteurs au sein de l'organisation. L'entité analysée, structure

ou projet, a son organisation interne et coopère avec d'autres entités pour remplir sa fonction. Les processus CobiT apportent ici un canevas de référence neutre, sur lequel on peut cartographier l'organisation étudiée. Pour chaque processus de la

fonction informatique, les auditeurs repèrent qui fait quoi.

Prenons l'exemple du processus « Acquérir l'infrastructure technologique et la maintenir », que CobiT recense dans le domaine « Acquisition et mise en place » de la fonction informatique. Le projet étudié a une cellule technique qui coopère avec les Achats pour référencer et acquérir les produits nécessaires. L'engagement budgétaire lui-même dépend de plusieurs signatures réparties dans plusieurs directions. Les composants techniques du projet doivent ensuite être exploités par une direction de l'Exploitation, qui les insère dans une infrastructure technique plus large.

Ce repérage assez simple permet de prendre un recul nécessaire face à un symptôme global, tel que « le service manque de réactivité » : l'auditeur posera ensuite aux bonnes personnes les questions clés sur l'efficacité du processus d'acquisition, pour analyser le niveau de coopération entre la cellule technique et les Achats, ou encore la qualité des dossiers d'instruction soumis aux signataires, leur niveau de familiarité avec le dossier, etc.

Il est à noter que la fonction Achats interviendra aussi, avec un rôle très différent, pour la sélection des prestataires intervenant sur le projet. Ce rôle sera repéré lorsque l'auditeur passe au processus « Acquérir des applications et les maintenir ».

Sur la trame du référentiel des processus CobiT, l'équipe d'audit dresse ainsi la carte des unités qui interviennent dans le projet. Elle place le périmètre étudié, nécessairement délimité, dans un contexte plus large. La carte obtenue fait apparaître les rôles, les frontières, les dépendances internes et externes qui seront structurantes dans la performance de l'entité étudiée. La liste des entretiens à programmer s'allonge alors brusquement, car l'équipe d'audit perçoit la « géopolitique » de son objet d'étude, parfois sensiblement différente de ce qu'exposent les premiers entretiens.

Dès cette étape, CobiT joue son rôle de référentiel : la liste des processus est certes fastidieuse, mais l'auditeur n'oubliera pas de fonction clé dans la complexité qu'il découvre derrière les implicites de ses interlocuteurs, qui en sont, eux, familiers. Il peut vite soupçonner que certains rôles ne sont pas assurés, ou s'interroger sur le trop grand nombre de « casquettes » d'un acteur unique : ce dernier peut-il remplir correctement toutes ses attributions ?

Par ailleurs, l'urgence exige souvent de mettre en place une équipe de plusieurs auditeurs. Le référentiel est la langue commune de l'équipe d'audit : il permet une répartition du travail précise. La redondance entre les auditeurs n'est jamais nulle, mais, bien maîtrisée, elle devient fructueuse pour affiner les constats.

La vue détaillée

Au stade des entretiens d'approfondissement, l'utilisation de CobiT devient beaucoup plus délicate. Le « Guide d'audit » est un redoutable manuel de 250 pages sur deux colonnes, dont le niveau de précision n'est pas compatible avec

l'urgence du diagnostic attendu par le commanditaire, ni même avec la conduite d'un entretien efficace.

L'équipe d'audit doit donc extraire du référentiel les questions clés. Elle est aidée dans cet exercice par l'étape de cartographie précédente, par son expérience propre, mais aussi par un autre support du référentiel CobiT, le « Guide de management ». Ce dernier énonce, en une page par processus, les *facteurs clés de succès*, les *indicateurs clés d'objectifs*, les *indicateurs clés de performance*.

Poursuivons l'exemple du processus « Acquérir l'infrastructure technologique et la maintenir ». Les facteurs clés de succès de ce processus, rappelés en encart, font apparaître les dimensions de pilotage et d'exécution de ce processus, ses enjeux à

court et moyen terme, les points où le processus se grippe parfois et qui seront donc l'objet de l'attention de l'auditeur.

Dans les études qui nous sont confiées, cette maille d'analyse, plus modeste, est appropriée pour construire des guides d'entretien maîtrisables et pour rechercher les informations déterminantes dans la documentation remise aux auditeurs.

Il reste cependant un domaine où le cadre de référence CobiT n'est pas l'outil d'analyse approprié : il s'agit de la gestion de projet. Ce domaine relève en fait de plusieurs processus du référentiel CobiT : « Gérer les projets », bien sûr, mais aussi « Evaluer les risques », « Trouver des solutions informatiques », « Acquérir des applications et les maintenir »,

Processus « Acquérir l'infrastructure technologique et la maintenir » Facteurs Clés de Succès

- L'encadrement supérieur apporte un soutien vigoureux à la méthode d'acquisition et de mise en place
- Les pratiques d'acquisition sont claires, comprises, et acceptées
- L'intégration entre les différentes plates-formes technologiques se fait facilement
- L'encadrement supérieur définit et défend une stratégie d'entreprise bien articulée avec les exigences d'architecture informatique qui en découlent
- On dispose d'un inventaire de l'infrastructure matérielle et logicielle à jour
- Les relations avec les fournisseurs sont bien développées
- On a la capacité de définir assez justement le coût de la redondance entre différentes plates-formes technologiques
- On a défini des politiques qui permettent de choisir rationnellement entre le développement interne, la mobilisation de structures externes, et l'externalisation
- Le processus de choix privilégie les composants réutilisables
- Les politiques sont définies de manière à gérer la dépendance vis-à-vis des fournisseurs exclusifs
- Les processus et systèmes de gestion des changements sont coordonnés avec le processus d'acquisition et de mise en place
- On utilise une méthode bien définie de cycle de vie pour choisir, acheter, entretenir et mettre hors service les composants système
- L'achat tient parfaitement compte des niveaux de performance et de capacité requis par les processus de gestion de performance et la capacité
- On dispose d'un ensemble d'outils d'assistance automatisés approprié, qui fait gagner du temps dans le choix des composants en permettant d'identifier d'emblée les plus aboutis

Extrait du « Guide de management CobiT », p.52.

« Développer les procédures et les maintenir ». Pour l'efficacité d'une intervention d'audit de projet, il est préférable de resserrer l'analyse sur un corpus des « bonnes pratiques » de gestion de projet, tel que ceux que l'AFNOR ou l'AFAI ont publiés.

L'apport d'un cadre structuré

Le référentiel CobiT apporte donc, dans notre pratique opérationnelle,

deux éléments importants : d'une part, une structure partagée entre les intervenants d'une équipe d'audit, qui doit explorer un territoire complexe sous la pression du délai convenu ; d'autre part, un quadrillage, parfois trop systématique, que les auditeurs exploitent comme check-list afin de préparer leurs propres outils.

Cette démarche exige un investissement d'appropriation important du

référentiel, qui n'est utilisable, pour des missions de ce type, qu'avec des adaptations importantes aux objectifs et aux priorités de l'audit.

Nous avons donc construit, au sein de Fontaine Consultants, un référentiel d'audit propre au type de missions qui nous sont confiées, qui permet à nos auditeurs de déployer leur expertise et de coopérer en équipes performantes.

LES OUVRAGES PARUS

■ La rentabilité des projets informatiques

L'étude de la rentabilité des projets informatiques, c'est un piège : « si on ne le fait pas, on vous le reproche ; et si on le fait, personne n'y croit. » Voilà le décor planté. Pourtant, cela n'est pas si difficile. Pour une direction générale ou un DSI, le pilotage des projets par leur retour sur investissement devrait être la règle. Force est de constater que ce n'est que trop rarement le cas, au mépris des saines règles de l'IT Governance.

Réhabiliter de saines pratiques en matière d'analyse de rentabilité, détailler une méthodologie, fournir des points de repère, illustrer la démarche par des cas concrets, et surtout mettre en filigrane de tout projet les critères de sa rentabilité pour établir des jalons, mesurer les points de contrôle, et décider au cours de la vie du projet, s'il passe l'examen de la décision, de continuer, de réorienter ou d'arrêter le projet sont les objectifs de cet ouvrage. Ambitieux, probablement, mais utile sans doute.

■ Le livre blanc sur l'enquête ERP

À l'occasion du séminaire du 18 janvier 2005, l'AFAI publiera un livre blanc qui résulte de l'enquête menée par ASK Conseil sur les bonnes pratiques observées en matière de mise en place d'ERP. Cette enquête a permis de mettre en évidence des typologies de comportement entre Groupes d'origine diverses (USA, UK, RFA, FR) sur deux grands ERP du marché, SAP et ORACLE.

Les auteurs en ont dégagé une voie de progrès concrétisée par un modèle de maturité pour réussir la transformation de l'entreprise en alignant la performance à la stratégie ERP.

LES OUVRAGES À PARAÎTRE

■ Le support client

L'ouvrage qui sortira au premier semestre 2005 est destiné à mettre en exergue le rôle déterminant de la fonction support dans le pilotage de la performance de l'informatique. En effet, les travaux sur le thème de la performance se polarisent sur les projets là où les budgets sont de plus en plus absorbés par les tâches récurrentes. Cet ouvrage permettra de :

- comprendre le rôle central du support dans une approche de gouvernance basée sur IT Scorecard ;
- réussir la greffe d'un contrat externalisé dans les processus internes et auprès des acteurs concernés ;
- passer en revue les méthodes (ITIL, CoBIT) et se situer vis-à-vis des bonnes pratiques (modèle de maturité, modèle d'évolution).

Son résultat sera une **boîte à outils** recensant les principales pratiques, les pistes possibles d'amélioration et les interrogations ouvertes.