Le retour du contrôle

Au-delà des problèmes de traduction

Martine Otter, Présidente d'ADELI

La version 2000 des normes ISO 9000 a fait disparaître les normes ISO 9002 et ISO 9003 qui faisaient la part belle aux dispositifs de contrôle. Les actions préventives de construction de la qualité, situées dans les phases les plus amont des processus de conception, ont alors été privilégiées. Le « contrôle » a été banni du langage des qualiticiens, pour laisser la place aux démarches préventives de l'assurance qualité, puis au management de la qualité. Bien mal leur en a pris, car le contrôle est revenu en force dans le discours des financiers.
COSO et CobIT, référentiels à usage des auditeurs, tiennent maintenant le haut du pavé et viennent outiller les législations telles que la Loi de Sécurité Financière et Sarbanes Oxley pour rassurer les actionnaires des entreprises.
Comment trouver un juste équilibre entre contrôle et prévention ?

Les précurseurs

Les pratiques de contrôle ne sont pas nouvelles. On cite souvent la Genèse comme premier exemple de contrôle qualité : après six jours de création, Dieu prend un peu de recul et « vit que cela était bon ». Contrôler consiste à vérifier la conformité d'un produit ou d'un processus à ses spécifications, lorsqu'elles sont définies. En l'absence de spécifications, le contrôle prend la forme d'un jugement d'expert dont l'objectivité est forcément contestable : nous ne connaîtrons jamais les critères du Créateur !

Dans le sens le plus étroit, contrôler c'est vérifier l'exécution des ordres donnés et c'est l'une des tâches essentielles de la fonction administrative, telle que la définit Fayol au tout début du 20ème siècle dans son ouvrage « *Administration industrielle et générale* ».

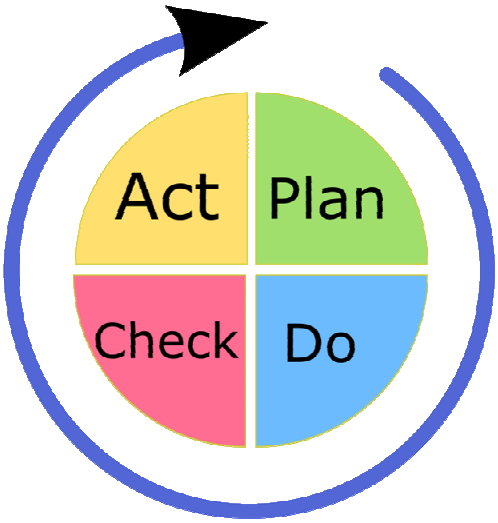

Figure 1 : La roue de Deming
ou principe d'amélioration permanente

La roue de Deming, également connue sous le sigle PDCA (Plan Do Check Act[1]) positionne les actions de vérification non plus dans le domaine de l'obéissance aux ordres mais sur celui de l'efficacité des actions décidées et exécutées. Le contrôle s'inscrit dans un cycle à quatre temps, dont il constitue le troisième temps.

Il s'agit alors de se livrer à une autocritique en règle des décisions prises lors du « tour de roue » précédent, afin de corriger les dysfonctionnements éventuels et d'améliorer encore le fonctionnement du système, entreprise ou processus particulier.

Point de traduction

Chaque fois que l'on prononce le mot contrôle au sein de l'entreprise, « on » vous explique qu'il faut bien sûr l'entendre au sens anglo-saxon du terme qui ne comporterait pas, dit-on, tout l'arrière plan négatif du mot contrôle en français.

Dans la langue française le contrôle est forcément tatillon ; il dénote une absence de confiance.

En anglais contrôler serait synonyme de maîtriser. « Les processus sont sous contrôle » signifierait qu'on les a bien en main, pas forcément qu'on passe son temps en vérification d'application de procédures. Si l'on ouvre un dictionnaire anglais, on constate cependant que le mot « control » peut prendre toutes les nuances, depuis celle du contrôle tatillon à celle de la maîtrise. En fait, le contrôle est naturel dans la culture anglo-saxonne.

Contrôle qualité

Contrôle du produit

Dans les premières versions de la norme ISO 9001 (1987, puis révision de 1994), les procédures de contrôle ont pour objectif de vérifier que « les

[1] *Planifier – Exécuter – Vérifier – Corriger*

exigences spécifiées pour les produits sont respectées ». Le contrôle doit apporter la preuve de la conformité : en matière de logiciel et de Système d'Information, les contrôles se traduisent essentiellement par des tests.

Contrôles et essais peuvent être exécutés à différents stades de réalisation d'un produit : dès la conception, en cours de fabrication ou seulement lors d'essais finals. Cette distinction était à la base de la différence entre les trois niveaux de certification.

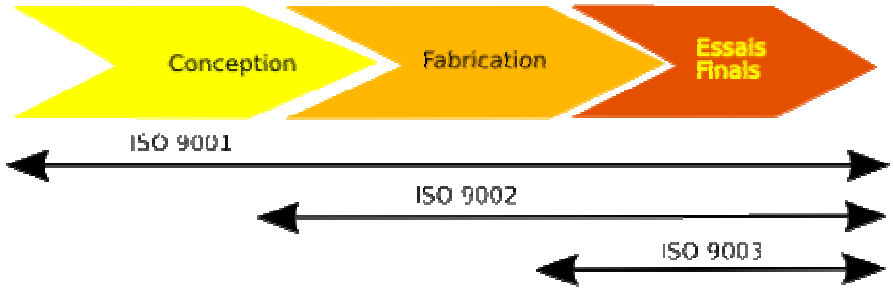

Figure 2 : Les 3 niveaux de certification version 1994

La qualité des contrôles est garantie à la fois par la vérification des équipements de contrôle et par la maîtrise de l'enregistrement des contrôles et essais.

Contrôle des processus

La vérification de l'aptitude des processus, bien que non décrite de façon explicite, est déjà présente dans l'ISO 9001 version 1987 : elle justifie la collecte de données et l'emploi de techniques statistiques (chapitre 4.20). Vérifier un processus consiste à s'assurer qu'il produit les résultats attendus de façon régulière.

La version 2000 de l'ISO 9000 a mis au premier plan l'approche processus : l'établissement d'une cartographie des processus de l'entreprise permet d'analyser l'ensemble des interfaces client-fournisseur, internes ou externes et d'en comprendre le mécanisme. Chaque processus concourt à l'amélioration globale de l'ensemble en s'inscrivant dans un PDCA général. Les actions de contrôle, tests et vérifications de toute nature, contribuent pour leur part à la maîtrise générale du système dont elles ne sont cependant que l'un des éléments.

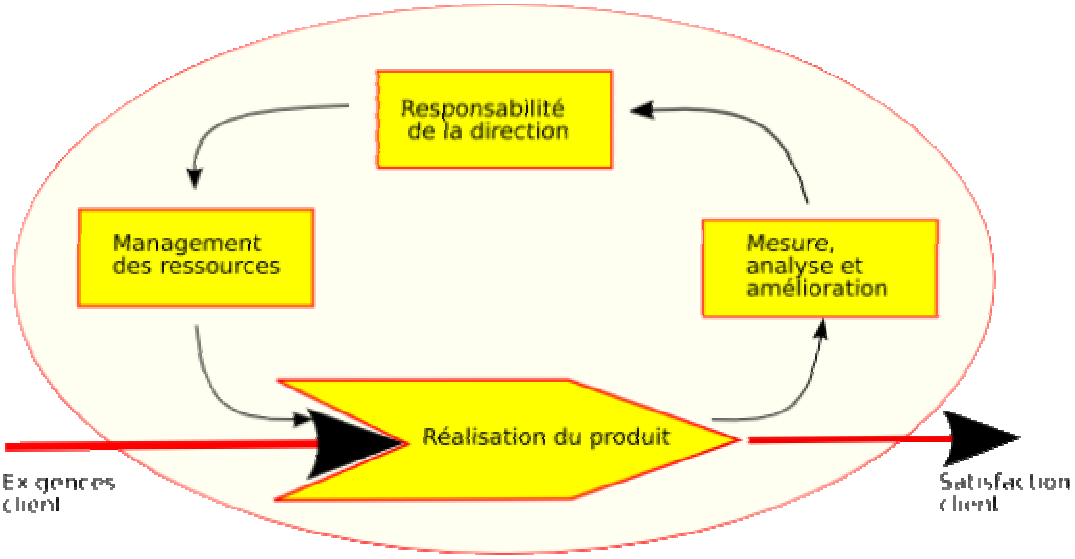

Figure 3 : Système de management de la qualité
Modèle de processus ISO 9000

Contrôle ou audit ?

Le troisième type de contrôle présent dans la série des normes ISO 9000 est l'audit qualité qui est une forme de contrôle soumise à des principes formels assez stricts. Le résultat de l'audit est une liste d'écarts assortis d'un niveau de gravité plus ou moins élevé.

L'objectif est de vérifier à la fois la conformité du Système Qualité à la norme et son efficacité : la norme doit être appliquée et cette application doit conduire à la satisfaction du client. La concordance

entre ces deux objectifs n'était pas toujours obtenue dans les versions 1987 ou 1994, ce qui a justifié en partie les évolutions de la révision 2000.
L'audit vient compléter de façon statique l'ensemble des contrôles effectués au fil de l'eau et de façon plus dynamique sur les processus. On peut résumer la différence entre ces deux types de pratique en disant que les contrôles sont exercés de façon quasi continue par le management, alors que l'audit est en principe effectué de façon ponctuelle par un tiers indépendant. En pratique, toutefois, le terme d'audit peut être utilisé dans des situations plus informelles, en l'absence de tout référentiel. Inversement les contrôles peuvent être encadrés par un référentiel, tel CobiT, qui en précise le contenu. Pour compliquer le tout, le terme « revue » est quelquefois utilisé pour édulcorer la notion de contrôle ou d'audit et ne pas susciter de réaction négative de la part du personnel.

Contrôle financier versus contrôle qualité

Le contrôle financier c'est l'affaire du contrôle de gestion et des commissaires aux comptes : il s'agit de garantir la véracité et l'exactitude des résultats comptables.

Il existe dans nombre d'entreprises plusieurs services d'audit : l'audit interne comptable d'un côté et l'audit qualité de l'autre, ce dernier pouvant s'étendre aux domaines de l'environnement et de la sécurité. Le qualiticien n'est généralement pas un spécialiste du contrôle de gestion de même que l'auditeur comptable n'a que rarement des compétences en matière de qualité. Les formations de ces deux types de professionnels se font dans des cursus différents.

L'auditeur financier est présenté par l'ONISEP (Office National d'Information Sur les Enseignements et les Professions) comme le Sherlock Holmes au sein de l'entreprise :

« Initié dans le secret des comptes d'une entreprise, l'auditeur financier doit détecter d'éventuels dysfonctionnements ou anomalies. Il veille à la santé financière des entreprises et traque les défauts d'organisation. Véritable enquêteur, il rencontre les dirigeants et cadres de l'entreprise, étudie les comptes de la société et les documents internes, examine les pièces comptables. Il collecte toutes les informations, parfois confidentielles, nécessaires pour analyser le fonctionnement de l'entreprise.
Qu'il soit rattaché à une société (auditeur interne) ou à un cabinet (auditeur externe), l'auditeur contribue à améliorer l'efficacité des différents services d'une entreprise. »

« L'auditeur qualité, de son côté, évalue la démarche qualité de l'entreprise, dont il peut faire partie ou non. Ainsi, l'auditeur externe vérifie que les moyens utilisés répondent aux normes de qualité en vigueur. Si tout est conforme, il délivre à l'entreprise une certification. L'auditeur interne, de son côté, analyse le fonctionnement de son entreprise, identifie les sources de non-qualité et propose des mesures correctives. »

Les deux définitions ci-dessus font apparaître un point commun essentiel entre les deux fonctions d'audit : audit financier et audit qualité visent tous deux à améliorer les processus de l'entreprise.

Le risque de cette double approche est bien sûr la redondance : l'analyse des processus peut conduire à des recommandations différentes, voire opposées. Il est dommage de construire deux cartographies des processus, l'une pour les besoins de la qualité, l'autre pour ceux du contrôle financier. Les structures qualité et financières sont généralement rattachées à des directions différentes, les deux structures hiérarchiques ne se regroupant qu'au niveau le plus élevé de la Direction Générale, qui a d'autres préoccupations que l'arbitrage entre contrôle financier et contrôle qualité…

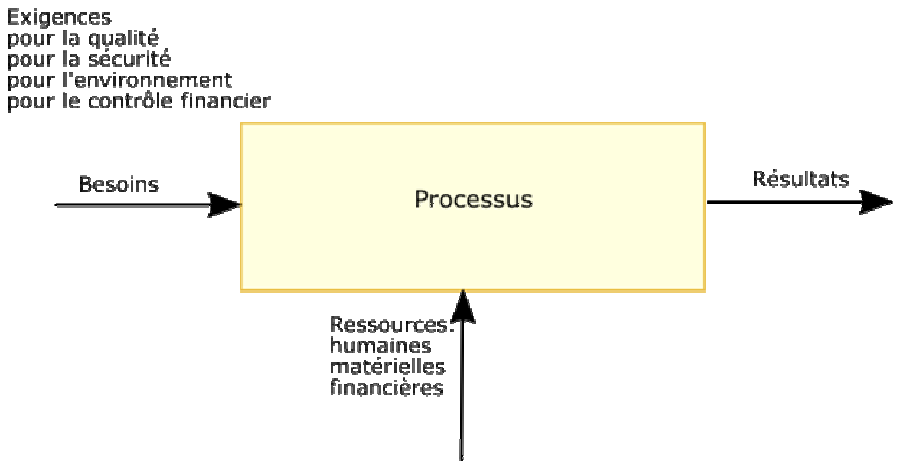

Figure 4 : Modèle de processus de base

Pourtant le modèle de processus est le même que l'on se place du point de vue financier ou du point de vue qualité. Les exigences auxquelles est soumis un processus doivent être arbitrées au cas où elles créeraient des situations conflictuelles : nous pouvons citer par exemple l'obligation de « whistle-blowing[1] », possibilité de signalement par un employé de pratiques illégales ou frauduleuses d'un autre employé ou manager, qui ne peut être mise en place dans une entreprise que dans le respect des réglementations de protection des données personnelles.

Si l'on veut répondre à la fois aux exigences du contrôle financier et du contrôle qualité, il convient de compléter ce schéma pour le rendre plus dynamique. Les processus doivent certes transformer des besoins en résultats, sous contrainte de ressources, mais une telle modélisation passe sous silence l'aspect temporel du processus et les aléas divers qui viennent mettre son déroulement en péril. La prise en compte des risques dans le modèle de processus permet de répondre aux besoins du contrôle financier comme à ceux du contrôle qualité.

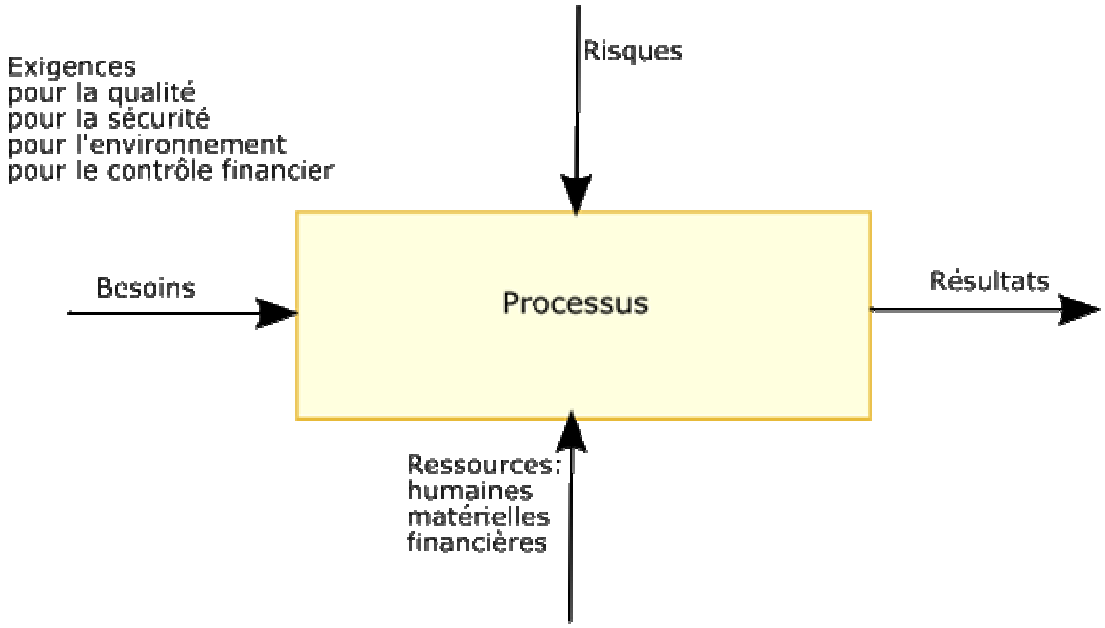

Figure 5 : Modèle de processus complété

Le management par les risques permet un rapprochement de ces deux approches du contrôle : le risque de fraude est-il un risque pour la qualité ou un risque pour la finance ? Les pratiques de bonne gouvernance concernent aussi bien les processus métiers que les processus comptables.

Des référentiels pour le contrôle

Des référentiels pour le contrôle existaient depuis longtemps mais leur usage n'était que peu répandu. Ce n'est qu'en 2002 aux États-Unis, suite à différents scandales financiers dont l'affaire Enron n'est que le plus célèbre, que la loi Sarbanes-Oxley est venue poser des exigences de contrôle, sans toutefois les définir.

Les référentiels pour le contrôle sont alors devenus incontournables et ont pris un essor sans précédent. Dans différents pays, les sociétés cotées en Bourse se sont vues soumises à une obligation de reporting auprès des autorités financières.

Nous présentons ci-après quelques-uns de ces référentiels, dont l'origine est systématiquement outre-Atlantique. Si quelque lecteur avait identifié un tel référentiel d'origine européenne, nous lui serions reconnaissants de nous le signaler !

En France, l'AMF (Autorité des Marchés Financiers), autorité publique indépendante issue en 2003 de la fusion de la Commission des opérations (COB) et du Conseil des marchés financiers, collecte les rapports rendus obligatoires par la Loi de Sécurité Financière, mais n'impose pas de contenu précis : le rapport doit simplement décrire les procédures de contrôle « sans être tenu de les évaluer ou d'apprécier leur adéquation ou leur efficacité ». Pour répondre à ce besoin, l'AMF a mis en place un groupe de travail composé

[1] *en anglais, dénonciation, littéralement « émission d'un sifflement » ; évoque la possibilité qu'a l'arbitre d'un match de football, par exemple, de mettre fin au jeu par un coup de sifflet.*

de représentants des entreprises, de professionnels de la comptabilité et de professionnels de l'audit interne pour parvenir à définir, d'ici fin 2005, un référentiel français de contrôle interne.

COSO

Contrairement à la législation française qui n'impose pas aux sociétés de se référer à un cadre normatif précis, la réglementation américaine impose un référentiel pour le contrôle interne : le COSO (Committee of Sponsoring Organizations of the Treadway Commission - www.coso.org), organisme créé en 1985 pour soutenir la « commission nationale sur le reporting financier frauduleux » !
Le COSO définit le contrôle interne comme un processus conçu pour fournir une assurance raisonnable dans l'atteinte des objectifs fixés dans les trois domaines suivants :

- réalisation et optimisation des opérations ;
- fiabilité des opérations financières ;
- conformité aux lois et réglementations applicables.

Ces objectifs recoupent largement ceux d'une démarche qualité. On notera simplement que l'aspect « amélioration permanente » y est moins présent, comme la fiabilité financière n'est pas explicitement énoncée dans l'ISO 9001. Dans les deux cas, il est nécessaire de cartographier les métiers de base de l'entreprise en les décomposant en processus. Dans les deux cas, la définition des activités de contrôle repose sur l'évaluation des risques.

SAS 70

Si vous êtes fournisseur de services auprès d'une société cotée en Bourse aux États-Unis, votre client vous réclamera probablement un rapport SAS 70. Ce référentiel de contrôle a été créé en 1992 par l'American Institute of Certified Public Accountants (AICPA) pour fournir un cadre de contrôle aux clients et auditeurs de sociétés de service.

Si on examine les exigences SAS 70[1], on y découvre un contenu similaire à celui d'un manuel qualité :

- description de l'organisation ;
- description des processus ;
- description des contrôles.

L'objectif affiché, comme dans le cas d'une certification ISO 9001, est de donner confiance au client sur votre capacité à lui fournir des services fiables et efficaces.

Les différences entre ces deux types de référentiel et de certification portent plus sur l'usage qui peut en être fait vis-à-vis des exigences du contrôle financier :

- Le rapport d'audit SAS 70 est fait pour être communiqué aux clients et auditeurs financiers externes, alors que le rapport d'audit servant de base à une certification ISO 9001 reste confidentiel,
- SAS 70 fournit un diagnostic précis sur les contrôles mis en place par l'entreprise vis-à-vis d'objectifs personnalisés, alors qu'ISO 9001 fournit un certificat global de conformité.

Si les démarches d'audit et de certification sont différentes, l'effort à mener est bien le même : une entreprise certifiée ISO 9001 devrait pouvoir fournir facilement un rapport SAS 70, à condition de maîtriser la langue anglaise. Réciproquement, le respect des exigences SAS 70 devrait faciliter la mise en place de la cartographie des processus requise par l'ISO 9001.

CobIT, un référentiel pour le contrôle de l'Information et des technologies associées

COSO ou SAS 70, tout comme ISO 9001, sont des référentiels génériques qui peuvent être utilisés dans tout type d'entreprise, pour tout type d'activité. En matière de système d'information, que l'entreprise se situe du côté utilisateur ou fournisseur, les contrôles doivent être définis dans des référentiels spécialisés qui prennent en compte les risques particuliers liés au traitement de l'information : perte d'intégrité, de confidentialité, rupture de service… Les experts-comptables n'étant généralement pas de formation technique doivent s'appuyer sur des « auditeurs de systèmes d'information », capables d'évaluer les risques du SI et d'investiguer au fin fond des PGI[2].

C'est ainsi que CobIT[3] a vu le jour en 1996. Il s'agit d'un référentiel construit pour les auditeurs « informatiques », dont on ne dit pas s'ils sont rattachés à la Direction financière ou à la Direction Qualité. Il leur fournit une démarche complète pour exercer leur activité de contrôle dans le domaine des technologies de l'information. L'audit n'est plus construit par rapport à un référentiel générique, comme c'est le cas dans l'ISO 9001, mais par rapport à des objectifs sélectionnés en fonction de la stratégie de l'entreprise. Une matrice de correspondance entre les contrôles requis par COSO, pour les besoins de l'application de la loi Sarbanes-Oxley, et les objectifs de contrôle CobiT a été défini par l'IT Governance Institute[4], afin de faciliter le passage d'un référentiel à l'autre.

[1] *http://www.sas70.com*

[2] *PGI : Programme de Gestion Intégrée (ERP en anglais)*

[3] *Pour une description plus complète de CobiT, on pourra se référer à l'ODOScope (©ADELI 2004) ou consulter le site de l'AFAI (http://www.afai.org) qui distribue CobiT en France.*
Un premier article de Claude Mauvais sur « le modèle Cobit » avait été publié dans La Lettre n°43 d'avril 2001.

[4] *http://www.itgi.org*

Conclusion

Les référentiels pour le contrôle financier et ceux pour la qualité visent en principe un même objectif, celui de l'amélioration des performances de l'entreprise, dans le respect de la législation en vigueur.

Les cultures au départ assez éloignées du contrôle de gestion et de la qualité tendent à se rapprocher dans un double mouvement, d'intégration des préoccupations d'efficience dans les référentiels qualité et, d'autre part, d'approche processus dans les référentiels de contrôle financiers.

L'outil majeur de ce rapprochement est le management par les risques : la non-qualité entraînant un défaut d'image et une perte de client est un risque à gérer au même titre que le risque de fraude ou de malversation financière. Le rôle du management est d'effectuer des choix pertinents en priorisant la réduction ou l'acceptation de tel ou tel risque en fonction de sa stratégie.

Espérons que ce rapprochement ne se fera pas au détriment de la satisfaction du client ou au seul bénéfice de l'actionnaire par une réduction drastique des coûts de fonctionnement. ▲

martine.otter@adeli.org