

communiqué

e-Commerce 2006 : tirer profit de la nouvelle donne

Quelles stratégies gagnantes pour saisir les nouvelles opportunités et faire face aux nouveaux défis ? Réponses des professionnels et experts au cours du nouveau forum Benchmark Group le 17 octobre à Paris.

LSF, Sarbanes-Oxley, Bâle 2 : quelles obligations ?

L'approche processus et l'approche risque sont complémentaires. Focus sur cette dernière au travers de qu'il ressort des textes de loi imposant des contraintes d'information nouvelles aux sociétés cotées.

19 Avril 2005

Consultant senior BPM, BPMS.
info

Suite à la débâcle d'Enron, annoncée en 2001, et à celle de nombreuses autres sociétés américaines ou européennes, des textes de loi sont venus dans la plupart des pays occidentaux apporter des contraintes d'information nouvelles aux sociétés cotées et éventuellement à d'autres sociétés commerciales.

Le site

■ [BPMS.info](#)

Deux grands objectifs communs caractérisent ces textes :

- détecter plus précocement les risques encourus par les actionnaires,
- et prévenir les comportements frauduleux des dirigeants, par des obligations de communication plus explicites et des peines encourues nouvelles ou aggravées.

C'est l'approche des risques d'une entreprise qui va retenir notre attention dans le présent article, tel qu'il ressort de textes aux abréviations désormais courantes : LSF, SOA et Bâle2.

La loi de Sécurité Financière (LSF)

La loi du 1er août 2003 sur la sécurité financière (LSF) couvre trois volets principaux : la modernisation des autorités de contrôle des marchés financiers, la sécurité des épargnants et des assurés et enfin le contrôle légal des comptes ainsi que la transparence et le gouvernement d'entreprise. Ce dernier volet s'adresse non seulement aux sociétés faisant appel public à l'épargne, mais à toutes les sociétés anonymes.

La LSF confie au Président d'une société la responsabilité de la rédaction et du contenu d'un rapport annuel sur les procédures de contrôle interne mises en place dans l'entreprise.

Ce volet de la LSF vise à imposer un usage étendu et très pragmatique du contrôle interne, dans une acception plus anglo-saxonne proche du contrôle des opérations (par opposition à une simple obligation formelle). Cette fonction renforcée du contrôle interne et des reportings associés doit permettre d'instiller une réelle culture de gouvernement d'entreprise entre les organes de contrôles (conseil d'administration ou de surveillance) et les organes de direction pour au final déboucher sur plus de transparence vis-à-vis des actionnaires.

La loi Sabarnes-Oxley

Le Sabarnes-Oxley Act (SOA) de 2002 concerne les seules sociétés cotées sur les marchés financiers nord américains auprès de la Security and Exchange Commission (SEC) et visait à sa création à apporter une réponse rapide à la crise de confiance en la fiabilité des informations communiquées par les entreprises. Le SOA est donc centré sur le contrôle de ces informations et il exige de surcroît que les directeurs généraux et directeurs financiers (CEO et CFO) engagent leur responsabilité sur la fiabilité de celles-ci.

L'article 404 traite des obligations liées au contrôle interne dans l'optique de la fiabilité de l'information financière délivrée, il introduit l'exigence d'un rapport d'évaluation de la qualité du contrôle interne dans l'entreprise, l'obligation (lourde) de documenter les tests de contrôle interne réalisés, et met un fort accent sur les dispositifs anti-fraudes. Cet article rend obligatoire l'utilisation d'un cadre d'analyse reconnu en matière de contrôle interne et cite en substance le référentiel COSO.

Ceci nous amène à nous arrêter quelques instants sur le cadre conceptuel du référentiel méthodologique COSO 2. Il se présente comme un cube dont les 3 dimensions sont :

1 Concourir à la réalisation des 3 objectifs suivants :

- la réalisation et l'optimisation des opérations,
- la fiabilité des opérations financières,
- la conformité aux lois et règlements.

2 Analyser pour chacun de ces 3 objectifs les 5 composantes du contrôle interne suivantes :

- l'environnement de contrôle,
- l'évaluation des risques,
- les activités de contrôle,
- l'information et la communication,
- le pilotage du contrôle interne.

3 Appliquer cette double approche à chaque activité et fonction de l'entreprise

COSO 2 promeut, sur la base de cette analyse en "cube", l'émergence de la notion de gestion des risques de l'entreprise, "l'Enterprise Risk Management ou ERM".

Cette gestion des risques doit être considérée dans une optique de pilotage : quels risques veut-on absolument éviter, quels risques sont inutiles, quels risques est-on prêt à prendre pour profiter de quelles opportunités ou conserver quel avantage ?

Il faut souligner à cette occasion qu'une organisation qui souhaiterait ne jamais prendre de risques se verrait par son immobilisme condamnée à disparaître.

Nous retiendrons à ce stade que, pour la LSF comme pour COSO 2, l'un des enjeux, (extrêmement positif) est d'amener l'entreprise à aligner sa stratégie et sa gestion des risques.

La réglementation dite "Bâle2"

Le dispositif réglementaire Bâle 2 concerne les établissements financiers européens, a été publié en 2004 et vise à une homologation des établissements par le régulateur en 2006. Il nous apporte des contraintes méthodologiques fort intéressantes en précisant des étapes de perfectionnement à suivre et en décomposant les risques par grande nature pour les établissements financiers : risques de crédit, risques de marché, et risques opérationnels.

Cette dernière catégorie retiendra plus particulièrement notre attention car c'est la moins spécifique au secteur bancaire, mise à part la nature de la récompense offerte aux plus méritants (la possibilité de diminuer la mobilisation de 15% de fonds propres sur les risques opérationnels de "l'approche de base" si la méthode suivie le justifie).

Le premier niveau de perfectionnement est "l'approche standard" pour laquelle il faudra :

- mettre en place un dispositif de collecte des incidents, avec une historisation longue et une consolidation le cas échéant (risques réalisés),
- découper les activités de la banque par ligne de métier,
- identifier les risques opérationnels de la banque, et dégager leurs composantes,
- évaluer les pertes potentielles liées à la réalisation de ces risques,
- définir des indicateurs de suivi des risques, construire et diffuser largement des reportings

internes sur les risques, et mettre en place des plans d'actions pour faire suite à ces reportings.

A ces premières obligations s'ajoutent pour "approche avancée" :

- mettre en place une entité indépendante, responsable de la gestion des risques opérationnels, des procédures et des contrôles,
- utiliser des données externes pour la prise en compte de risques extrêmes,
- calculer les fonds propres à mobiliser sur la base des incidents et des données externes collectés.

Deux démarches fortement imbriquées

On note de nombreux points communs entre COSO2 et la mise en œuvre d'un référentiel processus et les premières étapes d'une démarche projet seraient dans les deux cas identiques :

- comprendre et cartographier le ou les métiers de base de l'entreprise,
- les décomposer macro-processus métier ou support,
- puis en processus métier et processus support,
- obtenir la validation des organes de direction sur la pertinence de la représentation du tableau ainsi obtenu par rapport à leur connaissance de leur entreprise et de sa stratégie.

Sur cette base, un projet référentiel processus va poursuivre la décomposition "top down" jusqu'à parvenir à un niveau de détail par entité organisationnelle permettant d'éditer les procédures en vigueur, mais aussi de lister les applications informatiques touchées, les postes de travail concernés, tâche par tâche, éventuellement les compétences ou les systèmes de pilotage mis en oeuvre.

Comment intégrer les risques au référentiel

Un projet risques va devoir introduire une dimension ou une vue risques dans ce tableau et structurer les différentes caractéristiques des risques pour pouvoir les gérer (nature, probabilité, évaluation..).

La collecte des incidents selon Bâle 2 ou toute autre forme de recensement permettra de positionner chaque risque à un niveau adéquat, qui n'est généralement pas le niveau de granularité le plus fin d'une analyse référentiel processus.

Comparé à un projet de référentiel d'entreprise au périmètre maximal intégrant l'ensemble des prismes d'analyse des processus et du SI., le travail d'analyse, pour un projet strictement orienté "risques", apparaît considérablement allégé.

Tout d'abord, avec une démarche et des étapes intermédiaires très largement communes, et en dehors d'une course aux échéances de première mise en œuvre SOA ou Bâle 2, il serait vraiment dommageable pour une entreprise -notamment s'ils coexistent déjà- de ne pas lier ces deux projets dans la même base de donnée / référentiel.

On notera qu'insérer un projet risque au sein d'un projet référentiel processus offre une garantie de revue exhaustive de l'organisation et des processus sur le périmètre choisi.

Mais au-delà, les textes réglementaires n'ont pas vocation à produire de belles cartographies de risques mais bien à les maîtriser ou mieux, à les supprimer.

Les apports de l'intégration de la vue risques

Positionner un risque en haut de la pyramide des processus qui le génère (dans le cadre d'un projet processus), permet d'avoir immédiatement à disposition l'ensemble des procédures, acteurs, et systèmes concernés -autrement dit l'environnement de contrôle.

C'est tout de même la matière première, dans toute sa diversité, des changements nécessaires à la gestion du risque, qu'il s'agisse d'automatisation de tâches ou de contrôles, de formation ou de modifications de procédures.

La base de données référentiel apparaît aussi comme un outil indispensable pour "l'entité

indépendante" responsable de la gestion des risques opérationnels, des procédures et des contrôles de "l'approche avancée" de Bâle 2.

On ajoutera que positionner un contrôle dans un contexte qui permet d'identifier les ressources qu'il consomme permet d'en réévaluer rapidement le coût, et le cas échéant la pertinence, s'il n'est plus en rapport avec les bénéfices qui en sont attendus.

Cependant, insérer un projet risques dans un projet référentiel processus, si cela ne retire rien aux bénéfices précédemment décrits, ne suffit pas. L'obligation de documenter les contrôles nécessite plusieurs étapes supplémentaires :

- sélectionner des contrôles à effectuer au sein des systèmes opérationnels,
- les adresser à chacun des contrôleurs,
- suivre les contrôles et en conserver l'historique,
- générer documentation des rapports.

Toutes choses qui nécessitent de s'appuyer sur des outils complémentaires à la base de données référentiel (parfois proposés par les mêmes éditeurs), et des interfaces avec systèmes opérationnels en amont.

Tirer profit des contraintes réglementaires

En conclusion, plus les législateurs se sont adressés à des structures puissantes (cotées SEC) et homogènes (établissements financiers) plus ils ont pu être exigeants sur la définition d'un cadre d'analyse des risques poussant les entreprises à s'auto évaluer, pour aligner stratégie et profil de risques acceptés.

Nous aurions tendance à être encore plus ambitieux et à proposer d'utiliser les outils de modélisation de processus désormais matures pour appliquer la stratégie de façon cohérente non seulement avec la politique de risques, mais simultanément avec l'organisation des processus et avec toute autre dimension de ressource suivie dans la base de données.

Pour les dirigeants des entités qui ne sont pas concernées par SOA et Bâle 2, et donc avec moins de contraintes formelles sur les contrôles, mener un projet référentiel processus en intégrant la dimension risques peut s'avérer une façon extrêmement stimulante de rechercher une meilleure maîtrise de l'avenir de son entreprise, tout en recherchant pas à pas une utilisation plus rationnelle des ressources de l'organisation.

■ Laurent Hassid