# Un contrôle interne renforcé

*Le contrôle des systèmes d'information, y compris internet, demande une créativité permanente. Les organisations peuvent être modifiées, comme le montre la démarche de Crédit Agricole Indosuez.*

GIL DELILLE
*Responsable de la sécurité des systèmes d'information*
***Crédit agricole Indosuez***

L'observation du contrôle des risques des systèmes d'information des grands groupes internationaux fortement décentralisés entraîne des constatations diverses mais récurrentes :

- les règles de base sont parfois mal connues, surtout si l'on s'éloigne géographiquement et juridiquement du siège et la barrière de la langue peut constituer un frein au déploiement de ces règles ;
- l'organisation générale et les rôles individuels manquent parfois de cadre. Des Responsables de la sécurité des systèmes d'information (RSSIs) locaux, issus de l'informatique peuvent remplir un rôle officieux dans le processus de contrôle ;
- le siège du Groupe possède une visibilité partielle sur le niveau de sécurité réel et objectif des systèmes globaux. Les remontées d'informations restent parcellaires et focalisées sur des projets connotés «sécurité».

On observe un déploiement d'efforts identiques au sein d'entités qui communiquent peu et l'on voit les mêmes erreurs se répéter. La sécurité des données et des traitements est abordée sous un angle technique par la fonction informatique, qui, dans la majeure partie des cas, apprécie seule la nature des dispositifs de sécurité à déployer, trop centrés sur la disponibilité.

**«Le nombre élevé de correspondants, et la diversité de leur culture ont conduit à proposer une méthode d'analyse de risque unique et accessible à tous.»**

Face à ce constat, Crédit Agricole Indosuez a décidé, début 2000, de faire face à un nouvel enjeu : la mise en place d'une organisation fortement décentralisée et pourtant coordonnée par une cellule centrale spécialisée : la division des risques et de la sécurité des systèmes d'information.

## LES GRANDES LIGNES D'UNE APPROCHE DIFFÉRENTE

A ce stade, il est important de préciser que le code de sécurité de Crédit Agricole Indosuez stipule que le responsable des données confiées par la clientèle ou les partenaires est le responsable du métier concerné. Mais, ces responsables de métiers ne possèdent pas toujours de garanties formelles sur le niveau de confidentialité, disponibilité, intégrité et preuve des systèmes élaborés pour eux à leur demande.

Pour pallier ce manque, il a été décidé que chaque nouveau projet ferait l'objet d'un exposé des contraintes – commerciales, juridiques, réglementaires, techniques – et du besoin de sécurité y afférent. Selon le niveau de sécurité demandé, une analyse des risques pourra être produite. Un énoncé des souhaits du métier en termes de sécurité ou «cahier des charges sécurité» sera ensuite rédigé.

Nous avons rapidement réalisé qu'il était impossible d'obtenir ce type de dossier sans deux éléments majeurs : une méthode et un coordinateur. Compte tenu du nombre de projets décentralisés à l'intérieur de notre Groupe, il a été décidé que le coordinateur devait être implanté localement au sein de la filiale ou de la succursale. Ceci a donné naissance à un important réseau de correspondants. Le nombre élevé de ces correspondants, environ une quarantaine, et la diversité de leur culture ont conduit à proposer une méthode d'analyse de risque unique et accessible à tous. Leur mission comprend aussi la diffusion de la politique de sécurité auprès des utilisateurs et informaticiens, le contrôle de son application au quotidien et la mesure annuelle du degré de sécurité du secteur alloué.

Les correspondants constituent un réseau international coordonné par une cellule spécialisée, la Division des risques et de la sécurité des systèmes d'information (DRSSI). Celle-ci joue également un rôle support en fournissant documentation, modèles, outils et en favorisant les échanges d'expériences dans le Groupe. Afin de donner une dimen-

sion managériale au projet sécurité, la DRSSI a été rattachée au secrétariat général et un Comité de sécurité de l'information composé de membres de la direction générale discute, amende et entérine les textes proposés par la DRSSI. Parmi les textes figurent les différents volets de la politique de sécurité du Groupe. Il s'agit de recueils de règles applicables par les utilisateurs, les concepteurs et les exploitants du système d'information.

### De la théorie à la pratique

Crédit Agricole Indosuez a d'abord construit une base réglementaire cohérente, applicable à l'ensemble du Groupe. L'organisation globale, le rôle des correspondants, leur périmètre et leurs prérogatives ont été clairement définis. Ces dispositions nécessaires à la réussite du projet ont fait l'objet d'une publication par la direction générale et ont été relayées sur l'intranet du Groupe.

Cette base documentaire a été testée sur quatre filiales et directions pilotes, ce qui a amené à l'élaboration de documents complémentaires, tels l'illustration du rôle et du positionnement des correspondants, par exemple. Tous les documents ont simultanément été édités en langues française et anglaise, ce qui a conduit à des recrutements de personnes parfaitement bilingues afin de se doter d'une capacité de production équivalente en tous points en anglais et en français.

Le profil de l'équipe a été modifié. La connaissance des métiers de la banque est venue compléter des compétences techniques déjà élevées. Les produits de cette équipe – études, documentation, présentations – sont davantage en ligne avec les préoccupations des maîtres d'ouvrage.

Il a fallu simplifier la méthode d'analyse de risques. Après usage, nous avons constaté que le temps de production des dossiers d'analyse était encore trop long et nous avons conçu et programmé un «*workflow*». Un stock d'exemples d'analyses prêtes à la réutilisation est en cours de constitution. Rappelons que le but de ce projet est la généralisation de la pratique de l'analyse de risque à l'intérieur du Groupe.

Les canaux de communication ont été élargis, avec notamment la mise en place d'une base documentaire bilingue accessible à l'ensemble du Groupe, l'introduction de la sécurité dans des documents non dédiés à ce sujet (livret d'accueil de la DRH, portails intranet, fiches d'objectifs fournies par la DRH dans ses guides d'évaluation…). Enfin, lorsque le nombre de correspondants a atteint la masse critique, un séminaire d'information et de formation, bilingue lui aussi, a été organisé.

### Un modele de gestion homogene

Aujourd'hui, notre stratégie se résume à quelques postulats essentiels :

- une action orientée vers les maîtres d'ouvrage, c'est-à-dire les métiers ;
- une forte décentralisation et une forte responsabilisation de chaque métier et/ou filiale dans un cadre global défini par le siège ;
- la généralisation de l'énoncé du besoin de sécurité et de l'analyse des risques fournis en tant que base de travail aux maîtres d'œuvre ;
- une simplification maximale des méthodes et des messages ;
- l'utilisation de vecteurs de communication multiples ;
- une équipe internationale et intégrée.

Ce dispositif s'inscrit dans la logique de contrôle interne et de gestion du risque opérationnel de la banque. Il apporte la composante amont d'un processus démarrant dans le métier et aboutissant à l'adoption de mesures techniques, contractuelles, organisationnelles et prudentielles.

**«Le but est de généraliser la pratique de l'analyse de risque dans le Groupe.»**

La simplification et la généralisation des procédures d'analyse des risques visent à faire passer la banque d'un modèle de gestion ponctuelle du risque, typiquement internet et grandes applications (*graphique 1*) à un modèle de gestion homogène (*graphique 2*), où l'ensemble des projets, où qu'ils se déroulent et quelle que soit la technologie mise en œuvre, bénéficie d'un traitement local suivi depuis le siège.