CHAPITRE VII

LA SURVEILLANCE DES SYSTÈMES D'INFORMATIONS

1. Les activités en 2003
2. La collaboration internationale

1. Les activités en 2003

1.1. Entrevues et contrôles sur place

L'audit informatique a participé en 2003 à 114 entrevues et 3 contrôles sur place sur des sujets ayant trait au fonctionnement et à la sécurité des systèmes informatiques des entités surveillées. Un peu plus de la moitié des entrevues ont eu lieu avec des prestataires, consultants ou cabinets d'avocats.

L'audit informatique a également contribué à plusieurs séminaires ou conférences, réunions nationales dans le cadre de projets comme, par exemple, la mise en œuvre d'une autorité de certification nationale, et articles de presse.

A partir du mois de septembre 2003, l'audit informatique fut fortement sollicité par les entreprises désireuses de s'informer sur le changement de législation intervenu en août 2003. En effet, la loi du 2 août 2003, modifiant la loi du 5 avril 1993 relative au secteur financier, a entre autres introduit trois nouvelles catégories de professionnels du secteur financier (PSF) décrites aux articles 29-1, 29-2 et 29-3 de la loi du 5 avril 1993 dans le cadre desquelles se posent des questions relevant plus spécifiquement du domaine de compétence de l'audit informatique. Les activités couvertes par ces PSF, considérées comme connexes au secteur financier, ne reposent plus essentiellement sur la prestation de services financiers, mais sur la fourniture de services de sous-traitance en rapport avec l'activité financière. Il s'agit des statuts suivants :

- Les agents de communication à la clientèle dont les prestations couvrent notamment les services d'impression d'extraits de comptes ou de confirmations d'opérations financières ainsi que l'archivage des documents. La communication pouvant également se faire sous forme électronique, les titulaires de ce statut peuvent opérer des sites Internet consultatifs.

- Les agents administratifs qui peuvent contribuer aux processus métiers des établissements financiers et dont les prestations s'apparentent principalement à des fonctions de *back office*.

- Les opérateurs de systèmes et de réseaux de communication du secteur financier qui interviennent sur les systèmes informatiques des établissements financiers, mais qui ne peuvent pas intervenir au sein des processus métiers.

Le lecteur est invité à se reporter au chapitre 1er qui fournit de plus amples informations sur les particularités de ces activités.

L'audit informatique, dans le cadre de ces nouvelles activités, prend en considération le risque de concentration et se charge de vérifier le professionnalisme des activités, afin de s'assurer que la qualité des prestations réalisées en sous-traitance réponde aux mêmes critères que ceux des établissements financiers qui y font appel.

Un accent particulier est mis sur la ségrégation des environnements et des données. En effet, un prestataire chargé de traiter les travaux de plusieurs établissements financiers doit à tout moment pouvoir distinguer pour lequel d'entre eux il réalise une prestation. Il doit également être en mesure d'assurer une parfaite étanchéité entre les entités qu'il assiste, de manière à garantir à chacune une parfaite confidentialité des données confiées.

Lorsqu'une société ou un groupe constitue une nouvelle entité PSF et procède à un transfert partiel de personnel vers cette nouvelle structure, l'audit informatique veille au strict respect des droits d'accès aux locaux et systèmes, qui doivent être limités aux employés du PSF. En effet, une telle situation de transfert de personnel est souvent sujette à une difficulté de gestion du changement, particulièrement lorsque le PSF occupe des locaux adjacents à ceux de la société dont il est issu. Il n'est pas toujours facile et naturel pour les employés transférés de considérer leurs ex-collègues, qu'ils croisent éventuellement tous les jours du fait de la proximité des

locaux, comme des intervenants externes au sens de la circulaire IML 96/126. La circulaire précise, notamment, certaines pratiques à respecter en matière d'accès à l'environnement de production et de secret professionnel.

Etant donné l'origine des prestataires de services connexes, qui ne possèdent pas obligatoirement une «culture d'entreprise» analogue à celle d'un établissement soumis à la surveillance de la CSSF, l'audit informatique compte, dans un premier temps, mettre l'accent sur l'aspect pédagogique plutôt que répressif de la surveillance. L'objectif vise à transmettre aux nouveaux PSF les mécanismes de base qui régissent une gestion «saine et prudente» de l'activité. L'accent sera mis sur la pérennité des activités, l'élaboration des procédures, le principe des quatre yeux, ainsi que sur la ségrégation, l'intégrité et la confidentialité des données traitées.

1.2. Projet de recherche GRIF

La CSSF a signé en date du 30 juin 2003 une convention de collaboration avec le Centre de Recherche Public Henri Tudor (CRP-HT) qui porte sur la réalisation d'un projet de recherche appliquée, dénommé «Gestion des Risques Informatiques dans le Secteur Financier : nouvelles approches méthodologiques» (projet GRIF).

Ce projet, co-financé par le CRP-HT et la CSSF, s'inscrit dans le cadre de l'harmonisation internationale du contrôle bancaire telle que définie par le Nouvel Accord de Bâle («Bâle II») et en particulier en ce qui concerne la mission de surveillance de la CSSF au sein du «pilier 2» qui se concentre sur la revue par l'autorité de surveillance de l'adéquation du capital et du processus interne d'évaluation des établissements de crédit.

L'objectif majeur visé par la CSSF et le CRP-HT consiste à rechercher de nouvelles approches méthodologiques permettant d'évaluer, de préférence de manière quantitative, les risques liés à l'informatique. Il s'agit d'un domaine de recherche très spécifique, dont les résultats visent à formaliser et quantifier la prise en compte des risques informatiques au sein des risques opérationnels globaux des établissements financiers. Les connaissances rassemblées pour ce projet sont diverses et l'équipe de projet se compose à la fois de chercheurs du CRP-HT et d'agents de la CSSF, de manière à couvrir au mieux les domaines statistiques, mathématiques, informatiques, recherche documentaire, conduite de projet, audit de systèmes d'informations, surveillance prudentielle, sécurité des systèmes et finances.

Le projet GRIF s'étend dans sa phase initiale sur deux années et comporte quatre volets. Le premier volet consiste à créer une cellule de compétences sectorielles «informatique et finance», orientée vers la gestion des risques et la sécurité informatique. Le second volet porte sur la production d'un nouvel outil méthodologique, alors que le troisième volet consiste en une activité de validation des résultats en concertation avec les acteurs locaux. Le quatrième et dernier volet porte sur une étude de pérennisation et de valorisation des compétences, par exemple à l'aide d'un élargissement du partenariat avec les secteurs bancaire, institutionnel et informatique.

Fin 2003, l'équipe pluridisciplinaire de recherche a clôturé la phase de mise à niveau des connaissances. Ainsi, chaque membre dispose aujourd'hui d'une vision plus précise, tant sur les concepts de Bâle II que sur ceux de la gestion des risques informatiques. Les travaux à réaliser durant la prochaine phase porteront sur l'analyse des principales composantes qui entrent en ligne de compte dans le risque informatique. Il est probable qu'une représentation UML *(Unified Modeling Language)* permettra de mieux formaliser le modèle envisagé : ressources utilisées, propriétés de ces ressources, vulnérabilités et risques associés, etc. Ce genre de modèle pourrait aboutir à un langage ou à un formalisme commun aux établissements qui réalisent leur propre évaluation des risques dans le cadre de l'AMA *(Advanced Measurement Approach)* et à la CSSF qui doit valider leur approche.

2. La collaboration internationale

L'audit informatique participe aux travaux de l'Electronic Banking Group du Comité de Bâle (EBG). L'EBG a été constitué en novembre 1999 avec pour mission de réfléchir aux conséquences prudentielles des activités bancaires électroniques, principalement par Internet.

Le premier document intitulé «Electronic Banking Group Initiatives and White Papers» a été présenté en novembre 2000 et définissait l'initiative instaurée par le Comité de Bâle sur le contrôle bancaire.

Le document intitulé «Risk Management Principles for Electronic Banking», élaboré en mai 2001, a été publié sous sa forme définitive en juillet 2003. Il énonce les principaux points à respecter pour assurer une maîtrise adéquate des risques en matière d'e-banking, à savoir une gestion effective de la part des organes de décision des établissements financiers, des contrôles de sécurité (non répudiation, authentification, etc.), une gestion des risques légaux et des risques de réputation.

De même, le rapport «Management and Supervision of Cross-Border Electronic Banking Activities», publié pour la première fois en octobre 2002, qui, d'une part, identifie les responsabilités des établissements lorsqu'ils mettent en œuvre une activité transfrontalière par Internet, et d'autre part, précise les modalités de surveillance par les autorités respectives, c'est-à-dire celle ayant en charge l'établissement proposant le service et celle du pays d'accueil dans lequel le service est offert, a été publié sous sa forme définitive en juillet 2003. Ce document indique les limites d'une telle coopération entre autorités, particulièrement lorsque le pays d'origine ne prévoit pas de surveillance et que la prestation a lieu sans présence physique dans le pays d'accueil qui exige une surveillance pour l'activité prestée.

Aucun de ces deux documents publiés dans leur version définitive ne comporte de modification de fond. Les modifications portent essentiellement sur l'ordre de présentation de certaines notes de bas de page.

Durant l'année 2003, l'EBG a poursuivi son rôle de plate-forme d'échanges, permettant à ses membres de mieux cerner les enjeux actuels en matière de services e-banking. Il ressort de ces échanges d'informations, notamment dans le domaine de la cyber-criminalité, que certains continents, dont particulièrement l'Asie, subissent aujourd'hui une recrudescence d'apparition de faux sites bancaires *(fake web site)* destinés soit à induire l'usager en erreur afin de capter ses informations d'identification auprès des vrais sites ou de capter le numéro de cartes de crédit, soit à collecter de façon illicite des dépôts du public, alors que l'établissement de crédit n'existe pas. Ce thème de la sécurité des services financiers par Internet devrait être abordé par l'EBG en 2004, sous réserve de l'approbation du Comité de Bâle. Les enjeux de la sous-traitance *(outsourcing)* sont également envisagés comme thème à approfondir.