CHAPITRE VI

LA SURVEILLANCE DES SYSTÈMES D'INFORMATIONS

L'audit informatique de la CSSF a pour principale mission la surveillance prudentielle des systèmes d'informations, c'est-à-dire la prise en considération des aspects technologiques, essentiellement informatiques et de télécommunications, dans la surveillance du secteur financier. L'audit informatique s'intéresse aux risques opérationnels qui découlent de l'utilisation de systèmes informatiques par les établissements financiers et non pas aux risques financiers. Pour l'évaluation des risques opérationnels, l'audit informatique procède, lors de l'examen de projets soumis à la CSSF ou lors de contrôles sur place, souvent sur base d'une analyse comparative par rapport aux bonnes pratiques en matière informatique.

1. Les activités en 2002

1.1. Entrevues et contrôles sur place

En 2002, l'audit informatique a procédé à des entrevues et des contrôles sur place sur des sujets ayant trait au fonctionnement et à la sécurité des systèmes informatiques des entités surveillées. Les lettres envoyées aux établissements surveillés ont porté principalement sur des observations spécifiques aux projets présentés ou fait suite à des commentaires de la part des réviseurs externes dans leurs rapports ponctuels ou annuels.

Les principaux sujets couverts par les entretiens et contrôles sur place sont identiques à ceux observés en 2001, mais dans des proportions différentes.

- Les sites Internet restent d'actualité, mais les activités ou projets dans ce domaine sont globalement moins ambitieux. Ainsi, les nouveaux sites s'orientent davantage vers la messagerie sécurisée et la consultation par le client de ses actifs que vers la possibilité de passer des ordres en temps réel.

- La sous-traitance d'activités en relation avec l'informatique est croissante et vise simultanément une réduction des coûts grâce à une mise en commun des ressources nécessaires et une amélioration des prestations grâce à un personnel spécialisé dans l'activité sous-traitée.

- La délocalisation de systèmes auprès des maisons mères s'apparente en 2002 davantage à une activité de sous-traitance puisque l'objectif consiste à optimiser les compétences présentes dans le groupe en matière d'exploitation des systèmes.

- La définition des plans de continuité et des solutions informatiques de secours (backup) est un thème récurrent et stable par rapport à 2001, avec l'émergence de questions relatives à l'impact sur les risques opérationnels et leur évaluation dans le contexte du Nouvel Accord de Bâle.

- L'accès à distance (remote access) au site informatique par certains employés depuis leur domicile est un point émergeant soumis à la CSSF. Il est argumenté par une volonté de réduire les coûts tout en conservant la spécialisation des administrateurs de systèmes chargés d'intervenir (disponibilité et coût de transport). La sécurité est le principal élément critique à approfondir.

L'audit informatique est régulièrement approché par les sociétés informatiques ou cabinets-conseils qui sont en charge d'élaborer des projets pour les clients du secteur financier. Le dialogue initié en 2001 s'est concrétisé par 21 entretiens en 2002.

Il est important d'insister, comme par le passé, sur le fait que la CSSF ne donne aucun agrément à des entreprises qui ne sont pas sous son autorité et n'appose en aucune façon un label spécifique de conformité aux services prestés par ces sociétés qui ne peuvent se prévaloir d'une quelconque certification à la suite de tels entretiens.

1.2. Recensement des plans de continuité

La CSSF a procédé en 2002 à un recensement des plans de continuité, appelés en anglais «Business Continuity Plans» (BCP). Cette étude fait suite aux questions fréquemment posées depuis septembre 2001 en cette matière. Avant d'émettre d'éventuelles recommandations en la matière, la CSSF a souhaité dresser un état des lieux. Ce travail s'est concrétisé par un document intitulé «Recensement des BCP au 31 août 2002» qui a été adressé à tous les établissements de crédit et autres professionnels du secteur financier sous sa surveillance.

Le dépouillement des résultats est en cours d'achèvement et certaines caractéristiques sur un échantillon de 71 établissements de crédit de taille variable et 43 professionnels du secteur financier (PSF) sont d'ores et déjà mises en exergue.

- Les établissements de grande et moyenne taille ont globalement défini un BCP qui couvre l'ensemble des activités, supporté par une redondance importante des systèmes informatiques et de locaux spécifiques utilisables en cas de sinistre.

- Les établissements de petite taille, dont un nombre important de PSF, confondent BCP et «backup», c'est-à-dire qu'ils envisagent la continuité de leur activité principalement sur base d'un centre informatique de secours. Cette notion est en fait équivalente à celle de «Disaster Recovery Plan» (DRP) qui englobe les moyens de mise en œuvre d'un BCP. Cette approche peut se révéler incomplète si le BCP ne tient pas compte de l'ensemble des ressources nécessaires à l'activité, à savoir au moins le personnel et les locaux.

- Un nombre important d'établissements de taille moyenne ou réduite n'ont pas de BCP actuellement, mais ont initié un projet.

- Les établissements de taille moyenne ou réduite font massivement appel aux prestataires spécialisés dans la mise à disposition d'infrastructures informatiques de secours. Ces prestataires de centres de secours partagés ne sont pas nombreux et par conséquent, malgré le fait qu'ils permettent de mettre en place des solutions de «backup» à un coût moindre, ils représentent un risque de concentration en cas de sinistre assez important pour toucher plusieurs établissements financiers. Ce risque dépend également des différentes catégories de contrats et de leur répartition géographique par rapport au lieu du sinistre. L'établissement signataire du contrat le plus «faible» est davantage en situation de risque que les autres.

Dans certains pays, les autorités sont devenues normatives et imposent des distances minimales entre deux centres de traitement d'un établissement financier. La CSSF, dans ses réflexions, n'envisage pas encore de définir un critère de cette nature, particulièrement en raison des dimensions réduites du Grand-Duché et de la typologie de son infrastructure de communication qui fait apparaître un nombre réduit de nœuds stratégiques distants entre eux de moins de vingt kilomètres.

1.3. Autres faits marquants

La volonté de sous-traiter certaines activités est certainement le fait le plus marquant de l'année 2002. La CSSF a été consultée pour trois catégories de services de sous-traitance envisagés auprès de la maison mère ou d'une entité du groupe soumise à une autorité de surveillance du pays d'origine:

- les sites Internet consultatifs,

- les accès SWIFT dans le cadre de la migration SWIFTNet,

- la gestion de l'Active Directory Service au sein de Microsoft Windows 2000.

La circulaire IML 96/126 précise que les informations confidentielles ne peuvent être délocalisées hors du Luxembourg, particulièrement lorsqu'elles sont visibles par des tiers. L'analyse, au cas par cas, réalisée par la CSSF, fait ressortir les orientations suivantes :

a) Sites Internet consultatifs

Etant donné le coût élevé de l'architecture de sécurité à mettre en œuvre pour assurer une protection des réseaux connectés à Internet, certains établissements financiers de taille moyenne ou réduite ont exprimé le désir d'utiliser les infrastructures conséquentes de leur maison mère pour proposer un service consultatif à leurs clients.

Dans la mesure où aucune information transmise à la maison mère ne permet d'identifier le client, c'est-à-dire lorsque les états de compte ne comportent aucune information autre qu'un identifiant anonyme, et considérant que l'infrastructure et l'organisation envisagées sont conformes à l'état de l'art[1], la CSSF a admis ponctuellement le recours à la sous-traitance, en respect avec les contraintes énoncées dans la circulaire IML 96/126. La CSSF a également demandé aux établissements concernés une confirmation de la part de l'autorité de contrôle du pays où a lieu la prestation de sous-traitance, son accord pour la liaison informatique et une confirmation que les standards de sécurité utilisés sont adéquats.

b) Les accès SWIFT dans le cadre de la migration SWIFTNet

Le réseau SWIFT est un réseau à usage restreint aux professionnels du secteur financier dans le monde et a pour objectif de permettre la transmission d'ordres, sous forme électronique, de manière sécurisée et notariée (garantie de livraison), entre ses membres. Ce réseau constitue le moyen primaire le plus utilisé de communication entre établissements financiers du monde entier.

La société SWIFT a décidé de faire évoluer son réseau en adoptant le standard le plus répandu actuellement : le protocole IP spécifique à Internet. Cette évolution permet aux adhérents de recourir à des équipements plus répandus et plus facilement interopérables. Cette migration prévoit également par la suite l'utilisation de la signature électronique à l'aide d'une infrastructure à clés publiques (PKI, Public Key Infrastructure) et une modification des formats de messages avec l'adoption du standard ISO 15022, variante de XML. Le nouveau réseau porte le nom de SWIFTNet.

La CSSF a été confrontée à une demande d'établissements de crédit établis au Luxembourg, qui désiraient utiliser une plate-forme d'accès à SWIFTNet localisée auprès de leur maison mère. Ces établissements invoquaient un coût de migration élevé vers SWIFTNet qui pénaliserait leur activité au Luxembourg ; la solution alternative proposée consisterait à mutualiser l'infrastructure SWIFTNet.

Pour la CSSF, la mise en œuvre d'une infrastructure commune délocalisée hors du Luxembourg nécessite une étude plus approfondie.

L'usage d'une infrastructure commune localisée auprès d'un prestataire hors du Luxembourg, qu'il s'agisse de la maison mère ou d'une société proposant un «service bureau», suppose la transmission préalable du message SWIFT de l'établissement luxembourgeois vers le point d'accès SWIFT situé hors du territoire luxembourgeois. Techniquement, ces données qui contiennent le nom du donneur d'ordre, bien qu'elles transitent de manière cryptée, deviennent temporairement lisibles sur la station SWIFT avant envoi crypté dans le réseau SWIFT. Actuellement, un paramétrage inadéquat de la station SWIFT peut provoquer un stockage d'une durée plus ou moins longue sur cette station, en non-conformité aux dispositions de la circulaire IML 96/126.

[1] *Voir le rapport intitulé «Services financiers par Internet» réalisé par la CSSF en 2001.*

Avec SWIFTNet, il convient de distinguer la station SWIFT sur laquelle sont saisis les messages et le point d'accès, appelé «gateway», qui concentre les envois sur le réseau. La connexion entre la station et le «gateway» est spécifique à l'établissement et non à SWIFT. Si le «gateway» est localisé auprès d'un sous-traitant ou de la maison mère, le message transitera un instant sous forme lisible dans le «gateway» et l'établissement luxembourgeois devra alors s'assurer qu'aucun outil ni aucun individu – administrateur du système ou autre – n'est en mesure d'intercepter ces messages.

La délocalisation d'une plate-forme SWIFT représente par conséquent un risque de divulgation d'informations confidentielles et la CSSF étudiera des solutions afin d'écarter cet inconvénient.

Parallèlement, l'Association Luxembourgeoise des Membres et Utilisateurs SWIFT (ALMUS) analyse la mise en place au Luxembourg d'un «service bureau» qui consisterait en une alternative locale de mise en commun d'une infrastructure d'accès SWIFTNet de sorte que la communauté financière luxembourgeoise pourrait disposer, dans les délais imposés par SWIFT pour réaliser la migration vers SWIFTNet, d'une alternative locale de mise en commun des ressources informatiques pour autant qu'un ou plusieurs prestataires soient intéressés à proposer une telle activité.

c) La gestion de l'Active Directory Service au sein de Microsoft Windows 2000

Les utilisateurs du système d'exploitation Microsoft Windows 2000 ont à leur disposition un mécanisme de gestion des ressources – principalement les répertoires des utilisateurs – dénommé Active Directory Service (ADS) qui permet de gérer de manière centrale les droits d'accès des utilisateurs connectés en réseau. La particularité de l'ADS réside dans la possibilité d'administrer plusieurs réseaux par unité d'organisation géographique ou logique (business unit) à partir d'une arborescence.

Certains établissements luxembourgeois, appartenant à des groupes internationaux qui ont déployé Windows 2000 à travers toutes leurs entités, dans le but d'aboutir à une gestion homogène et simplifiée de ces ressources informatiques, ont adressé à la CSSF une demande portant sur la possibilité d'administration de l'ADS par la maison mère.

Compte tenu du fait que l'administrateur principal de l'ADS, qui dispose de la fonction «root», est en mesure de créer et de modifier les droits d'accès de n'importe quel utilisateur défini dans une arborescence, il est donc potentiellement capable d'accéder n'importe quelle ressource qui y est définie. Considérant que le réseau local d'un établissement financier est susceptible de contenir des données hautement confidentielles (lettres à des clients, recommandations stratégiques, contrats, etc.) stockées sur un ou plusieurs serveurs de fichiers ou serveur de messagerie électronique interne, il est primordial pour cet établissement d'avoir le plein contrôle sur les droits d'accès de ses ressources. Si un administrateur système tiers, délocalisé hors de l'établissement luxembourgeois, est en charge de la gestion de l'ADS et a accès à des possibilités qui lui permettent de contourner les mécanismes de sécurité en place et d'accéder en lecture aux ressources confidentielles, l'administration centralisée ne sera pas autorisée.

La CSSF rappelle qu'au-delà des obligations de secret professionnel, les établissements financiers sont tenus de maîtriser l'entièreté de leurs activités, y compris celles sous-traitées. Les aspects de sécurité qui conditionnent les modes d'utilisation des ressources informatiques doivent être sous contrôle de l'établissement financier.

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.

En mai 2001, l'EBG publiait les résultats des réflexions concernant les risques associés aux prestations bancaires par Internet. Le document intitulé «Risk Management Principles for Electronic Banking» énonce les principaux points à respecter pour assurer une maîtrise adéquate des risques en matière d'e-banking : 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.

A la suite de ces documents, l'EBG a décidé de se concentrer sur les aspects transfrontaliers de l'activité bancaire par Internet. Ainsi, en octobre 2002, l'EBG publiait le rapport «Management and Supervision of Cross-Border Electronic Banking Activities» qui, d'une part, identifie les responsabilités des établissements lorsqu'ils mettent en œuvre une activité transfrontalière par Internet, 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. Le 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.