CHAPITRE VIII

LA SURVEILLANCE DES SYSTEMES D'INFORMATIONS

1. Les activités en 2005

2. La pratique de la surveillance

1. LES ACTIVITES EN 2005

1.1. Entrevues et participations aux groupes nationaux

L'Audit informatique a participé en 2005 à 127 entrevues qui peuvent se catégoriser ainsi :

- entrevues en relation avec l'instruction de dossiers d'agrément pour l'exercice d'une activité de PSF de support, ceci en collaboration avec les autres services concernés,
- entrevues portant sur des sujets ayant trait au fonctionnement et à la sécurité des systèmes informatiques des entités surveillées, dont une majorité disposant d'un statut de PSF «opérateur de systèmes informatiques et de réseaux de communication du secteur financier», selon l'article 29-3 de la loi modifiée du 5 avril 1993 relative au secteur financier,
- entrevues avec des sociétés qui prestent des services au secteur financier afin de qualifier leurs activités et de déterminer si un agrément est requis ou non.

Ces entrevues ont eu lieu avec des sociétés offrant des services de sous-traitance au secteur financier, des sociétés de services en informatique, des cabinets d'avocats, des sociétés de conseils, des cabinets de révision et des entités surveillées.

L'Audit informatique a également participé à deux conférences internationales en qualité d'orateur et a assisté à seize séminaires ou conférences nationales portant sur des sujets en relation avec la sécurité des systèmes d'informations.

Les travaux relatifs à l'ISO au sein du Comité de Normalisation de la Sécurité de l'Information (CNLSI) se sont poursuivis, de même que ceux liés à l'élaboration d'un Master professionnel en «Management de la Sécurité des Systèmes d'Informations» (MSSI) en collaboration avec l'Université du Luxembourg et le Centre de Recherche Public Henri Tudor (CRP-HT). Il est à noter dans ce contexte que l'Audit informatique participe à deux Comités d'accompagnement stratégique mis en place par le CRP-HT pour déterminer les axes de recherches à investiguer dans les domaines de la Qualité et de la Sécurité des systèmes d'informations.

1.2. Projet de recherche GRIF

Le projet de recherche GRIF a débuté en 2003 en collaboration avec le Centre de Recherche Public Henri Tudor et porte sur la réalisation d'un projet de recherche appliquée renommé au cours de l'année 2005 «Gestion des Risques dans les Institutions Financières»[1].

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 II 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 à quantifier la prise en compte des risques informatiques au sein des risques opérationnels globaux des établissements financiers.

Fin 2004, la CSSF et le CRP-HT ont défini une méthodologie normée qui ne couvre plus uniquement les risques opérationnels informatiques, mais qui peut s'étendre à tout le volet du risque opérationnel tel qu'appréhendé dans Bâle II. De ce point de vue, les résultats du projet dépassent les objectifs initiaux et ont amené à revoir le titre du projet de manière à refléter l'étendue plus vaste couverte par ce modèle.

[1] Le titre initial était «Gestion des Risques Informatiques dans le Secteur Financier».

Le modèle retenu se base sur la norme ISO/IEC 15504 qui permet d'évaluer la maturité de processus. Dès lors que ces processus portent sur les risques, le modèle pourrait contribuer à répondre au nouveau cadre de la surveillance prudentielle sans imposer de contraintes sur des procédures spécifiques, mais en favorisant la valorisation du savoir-faire des institutions financières, de leurs fournisseurs (de conseils, de produits et de services), ainsi que des autorités de surveillance.

Les travaux réalisés au sein du projet GRIF ont permis de mettre en avant les avantages de la norme ISO/IEC 15504 qui permet l'évaluation de tous types d'organisations sur base de la maturité de ses processus et qui peut donc être appliquée par les institutions financières pour évaluer la maturité aussi bien de la gestion des risques opérationnels que des activités métiers. L'avantage indéniable de la norme ISO/IEC 15504 est de s'intéresser aux résultats attendus (le «quoi») et non à la manière de les atteindre (le «comment»), qui est laissé à la discrétion des acteurs, mais qui peut néanmoins reposer sur des pratiques de base communément acceptées et reflétées alors dans les questionnaires d'évaluation.

La recherche réalisée au sein du projet GRIF a porté sur l'établissement d'un modèle de référence des processus (*Process Reference Model*, c'est-à-dire un «PRM») construit sur base des critères énoncés par le Nouvel Accord de Bâle en matière de risques opérationnels. La traçabilité obtenue est bidirectionnelle et permet de valider l'origine dans Bâle II des processus à évaluer. Le modèle d'évaluation des processus (*Process Assessment Model* ou «PAM») a été élaboré par la suite, mais afin de pouvoir effectuer les évaluations, il reste à construire les questionnaires d'évaluation qui doivent également contenir les pratiques de base à respecter.

Pour la CSSF, les résultats actuels du projet, appliqués au contexte du pilier II de Bâle II, pourraient permettre l'obtention d'une mesure objective du modèle de gestion des risques opérationnels soumis par les établissements.

Fin 2005, après la présentation du projet GRIF aux acteurs concernés de la place, il apparaît que le principal attrait du projet consiste à avoir montré l'applicabilité de la norme ISO/IEC 15504 au sein du secteur financier, comme outil d'évaluation et d'amélioration des processus, qu'il s'agisse de processus métiers ou de processus de gestion des risques. Les acteurs intéressés de la place financière ainsi que le CRP-HT et la CSSF identifient plusieurs domaines d'utilisation potentiels de la norme ISO/IEC 15504 au sein du secteur financier, la liste n'étant pas exhaustive :

- dans le domaine de la sous-traitance, afin de mesurer l'aptitude d'un prestataire à délivrer ses services
  - pour les métiers des fonds d'investissements ou banque dépositaire, par exemple, en construisant des PRM «métiers» et les PAM associés,
  - pour les métiers de l'informatique, avec le projet AIDA[2] qui aboutit à la construction d'un PRM et d'un PAM portant sur ITIL[3] et qui permettrait d'évaluer la capacité des prestataires, y compris les PSF disposant du statut d'opérateur de systèmes, à mettre en œuvre ITIL.
- dans le domaine de l'audit, en établissant un PRM et un PAM spécifiques
  - aux contrôles internes,
  - à l'application des normes comptables IAS,
  - aux obligations légales, qu'il s'agisse de la mise en œuvre de nouvelles fonctions (fonction compliance par exemple), de la gestion des risques (pilier I) ou encore de la fonction informatique (circulaire CSSF 05/178).

L'intérêt de la méthode réside dans l'évaluation normative qui induit une cohérence des résultats et offre par conséquent la possibilité d'être réalisée par une tierce partie pour déterminer le niveau d'aptitude d'une organisation à gérer ses processus (ou ses risques opérationnels dans le contexte de Bâle II) et ceci de manière répétable.

[2] «Assessment and Improvement Integrated Approach», projet du CRP Henri Tudor (www.crpht.lu).

[3] IT Information Library (ITIL) est un ensemble de bonnes pratiques utilisées dans le but de délivrer des services informatiques de haute qualité.

Une auto-évaluation est également possible par ou pour le compte d'une organisation pour déterminer la pertinence de ses propres processus et les améliorer en vue d'un objectif particulier ou d'un ensemble d'exigences (pilier I de Bâle II).

Une documentation complète du projet GRIF est disponible sur le site de la CSSF (www.cssf.lu) à la rubrique «Dossiers», sous-rubrique «Adéquation des fonds propres», section «Le projet GRIF : Gestion des risques opérationnels dans les institutions financières».

1.3. Collaboration internationale

L'Audit informatique a participé à la conférence *International Supervisory Group on IT* qui réunit chaque année les responsables de la surveillance prudentielle des systèmes d'informations des différentes autorités[4]. Ce groupe a pour objectif de favoriser l'échange d'informations concernant les enjeux technologiques du moment et couvre des aspects comme les plans de continuité d'activités, l'*electronic banking*, les parades au phénomène de *phishing*[5] et la surveillance de la sous-traitance informatique transfrontalière. Tout au long de l'année, les membres du groupe échangent des informations concernant les fraudes liées à l'informatique et à Internet, les attaques de systèmes d'informations et le vol d'identité ou encore les faiblesses de certains systèmes.

2. LA PRATIQUE DE LA SURVEILLANCE

La surveillance porte sur la vérification de l'application du cadre légal et réglementaire par les entités surveillées, dans le but direct ou indirect de maintenir ou d'améliorer le professionnalisme des activités, avec un accent particulier sur les aspects liés aux technologies mises en œuvre en matière de systèmes d'informations et en tenant compte des particularités propres aux PSF connexes (aussi dénommés PSF de support) qui offrent leurs services de sous-traitance aux autres établissements surveillés.

2.1. Rappel des considérations prudentielles fondamentales

Concernant la surveillance des PSF de support, la CSSF invite le lecteur à se rapporter au Chapitre VII, point 2.1 du rapport d'activités 2004 de la CSSF qui précise l'importance de la ségrégation des environnements et des données des clients (les professionnels financiers). En effet, l'Audit informatique considère comme crucial pour un PSF de support d'assurer l'étanchéité entre les différents environnements, ceci quelles que soient les options technologiques retenues pour mutualiser les ressources. De plus, le principe prudentiel de ségrégation des fonctions, qui améliore les contrôles, permet de réduire les erreurs ou les fraudes et est fortement présent auprès des professionnels financiers, doit également se retrouver auprès des prestataires, qu'ils disposent d'un statut PSF de support ou non. L'Audit informatique insiste sur l'importance de la mise en place de ce principe prudentiel au sein des PSF de support et, en particulier, des opérateurs de systèmes informatiques et de réseaux de communication du secteur financier.

La CSSF constate également un écart culturel relativement important entre certains PSF de support, disposant du statut d'agent de communication à la clientèle ou du statut d'opérateur de systèmes et de réseaux, et les professionnels financiers qu'ils servent. Cette différence de culture se traduit par une compréhension souvent insuffisante des règles déontologiques spécifiques au secteur financier et, en particulier, par l'usage commercial, voire publicitaire, qui est fait de l'agrément ministériel. Les termes de l'article 52(3) de la loi modifiée du 5 avril 1993 sont pourtant explicites : «Nul ne peut faire état à des fins commerciales de son inscription sur un tableau officiel et de sa soumission à la surveillance de la Commission».

[4] Le groupe portait initialement le nom de «HITS» (Head of IT Supervision). Sont présentes les autorités des pays suivants : Etats-Unis, France, Belgique, Pays-Bas, Luxembourg, Italie, Espagne, Singapour, Hong Kong, Australie, Canada, Allemagne, Norvège et Angleterre (la Suède et la Suisse étant absentes en 2005).

[5] Phishing = (Phreaking + Fishing). Phreaking : hacking des centrales téléphoniques, depuis la blue Box de John Draper dans les années 70. Fishing : allusion à la pêche aux mots de passe dans l'océan Internet.

Il appert que de nombreux PSF de support assimilent incorrectement l'agrément et la surveillance associée à une certification ou un label de qualité. L'agrément a cependant pour principale conséquence d'imposer un cadre légal et réglementaire identique à celui applicable aux professionnels financiers. Il s'agit d'une obligation légale afin de pouvoir exercer cette activité et non d'une reconnaissance volontaire. Le fait de faire valoir de manière trop visible et commerciale l'agrément ministériel vis-à-vis des professionnels financiers, potentiels clients, peut aboutir à l'effet inverse de celui recherché lorsqu'il traduit ainsi ce clivage déontologique constaté par la CSSF.

2.2. Clarifications apportées suite à certaines questions posées

2.2.1. Accès distants : utilisation par une entité surveillée de la messagerie mobile «push-mail» et du produit «BlackBerry»

Une solution «push-mail» repose sur une infrastructure de messagerie qui fait appel à un ou plusieurs opérateurs mobiles pour véhiculer des messages électroniques de la messagerie interne de l'entreprise vers un équipement mobile, et vice-versa. Ce type de messagerie repose sur le principe de proactivité de l'équipement mobile, qui interroge très régulièrement le serveur de messagerie afin de récupérer d'éventuels messages en attente de transfert. Tout se passe comme si le serveur contactait l'équipement mobile lorsqu'il a des messages en attente, d'où le terme de «push-mail». Les équipements mobiles doivent donc être à même de faire fonctionner des programmes spécifiques aux fonctions «push-mail» ; c'est pourquoi ces équipements sont actuellement des téléphones mobiles possédant un système d'exploitation évolué (type Symbian par exemple) ou des PDA[6] dotés de fonctionnalités de téléphonie, qui communiquent à l'aide d'une connexion GPRS ou UMTS des opérateurs de réseaux GSM.

Afin de déterminer les critères de sécurité à respecter pour recourir à une solution «push-mail», il est nécessaire de qualifier l'information qui va transiter du professionnel financier à l'équipement mobile. Cette information est, *a priori*, considérée par la CSSF comme confidentielle puisqu'elle est issue du système de messagerie interne à l'entreprise et contient immanquablement à un moment donné des références à des clients. Par conséquent, la solution doit garantir une confidentialité et, de préférence, l'intégrité des informations échangées entre le serveur «push-mail» et l'équipement mobile.

De ce fait, le serveur «push-mail» doit être sous le contrôle exclusif du professionnel financier et donc dans ses locaux au Luxembourg.

Le recours incontournable aux opérateurs mobiles impose également une cryptographie des données échangées.

L'utilisateur mobile doit également être identifié par le serveur afin d'être certain qu'il est bien habilité à voir ces données confidentielles. Le seul recours au code secret d'activation de la carte SIM[7] peut ne pas suffire, en particulier si l'utilisateur non habilité remplace la carte SIM d'origine par une carte dont il connaît le code secret. La solution devra donc prévoir un code secret spécifique ou être reliée à la carte SIM de l'utilisateur habilité.

Enfin, si l'équipement mobile est perdu ou volé, les données qu'il contient ne doivent pas pouvoir être lues par un tiers et devront donc être fortement cryptées et, de préférence, pouvoir être effacées à distance.

La plus connue des solutions de «push-mail» a été conçue par la société anglaise Research In Motion Ltd (RIM) et se nomme BlackBerry®.

De nombreuses entités surveillées par la CSSF se sont enquises des possibilités ou restrictions d'usage de la solution BlackBerry®.

[6] PDA : Personal Digital Assistant (ordinateur de poche, à système d'exploitation Palm OS ou WindowsCE et dérivés).

[7] Carte à puce fournie par l'opérateur mobile.

Etant donné que les équipements mobiles et le serveur sont fournis par la société RIM, sachant que tous les messages transitent par une plate-forme informatique de RIM au Royaume-Uni, et à défaut pour ladite société de fournir des certifications de tiers de très haut niveau qui attestent des mécanismes de sécurité qu'elle énonce et de l'impossibilité pour des tiers, y compris elle-même, de déchiffrer les données transmises, la CSSF recommande une certaine prudence quant au recours à cette solution. Néanmoins, la confiance accordée à la société RIM fait l'objet de vérifications de la part de certains Etats, dont les Etats-Unis d'Amérique et la France, qui utilisent cette solution au plus haut niveau de l'Etat et des entreprises. Les certifications devraient donc être bientôt disponibles, à charge pour les professionnels financiers de vérifier la couverture de celles-ci et de déterminer la confiance à accorder à cette solution.

Certaines règles d'implémentation sont cependant à respecter. D'une part, le professionnel financier devra au moins recourir à l'option proposée par RIM qui consiste à permettre au professionnel financier de gérer lui-même les clés de cryptographie et, d'autre part, il devra disposer de la fonction d'effacement à distance des messages stockés sur les équipements mobiles perdus ou volés.

Aussi longtemps que les professionnels financiers gèrent eux-mêmes leur infrastructure BlackBerry®, cette solution n'est pas à considérer comme sous-traitance et un accord préalable de la CSSF n'est pas nécessaire.

2.2.2. Services de monitoring effectués par un prestataire sans statut de PSF de support

La CSSF confirme que les services de monitoring, qu'il s'agisse de surveillance d'applications, de systèmes informatiques ou de réseaux, ne sont pas considérés comme des services d'opération et ne relèvent pas d'un agrément dès lors que le prestataire ne dispose d'aucun moyen d'intervention sur les équipements surveillés.

La condition *sine qua non* à la fourniture de tels services sans agrément consiste à imposer contractuellement et opérationnellement l'intervention du client du prestataire pour prendre les actions correctrices nécessaires. Dans ce cas, le professionnel financier décide des actions à réaliser à la suite du monitoring et doit contrôler les actions du prestataire conformément aux indications énoncées dans la circulaire CSSF 05/178.

2.2.3. Cryptographie des lignes à très haut débit reposant sur la technologie de fibres optiques

L'évolution des télécommunications permet de disposer de lignes de transmission à très haut débit qui reposent sur la technologie des fibres optiques et qui permettent de réaliser des connexions entre unités centrales au niveau des processeurs de manière à rendre possibles des traitements véritablement «multi-processeurs» à distance. Ainsi, il devient possible de diviser la charge de travail des unités centrales sur des distances de plusieurs kilomètres, en assurant de cette sorte une redondance des équipements en cas de désastre sur l'un d'eux.

Le principal inconvénient de ces technologies consiste à rendre très coûteuse, voire prohibitive, toute cryptographie de ces canaux de communication à très haut débit, alors que la CSSF demande une protection des communications entre le professionnel financier et le centre de traitement distant.

Au cas où il ne serait techniquement pas possible, ou disproportionnellement onéreux, de crypter la ligne ou les données, le professionnel financier doit néanmoins s'assurer qu'aucun tiers, et en particulier aucun fournisseur d'accès aux lignes de télécommunication qui ne serait pas soumis par la loi au secret des communications, n'ait un accès non contrôlé aux données qui transitent par cette ligne. Les spécificités des fibres optiques permettent cependant d'envisager un contrôle de l'intégrité de la ligne qui reposerait sur une identification et une justification par tous les prestataires impliqués dans la fourniture de cette ligne, de toute rupture de communication.

En effet, il est extrêmement improbable pour un tiers de se connecter ou de tracer le contenu des données échangées sur ce type de ligne, sans devoir agir physiquement sur le réseau et provoquer dans ce cas une rupture temporaire de la fibre optique.

La CSSF invite cependant les professionnels financiers :

- d'une part, à envisager des solutions qui prévoient une cryptographie en amont de chaque service, en fonction de la criticité des données échangées, ce qui revient à ne pas crypter la ligne dans son ensemble, mais à crypter seulement les différents flux qui se concentrent sur la ligne (multiplexage logique des flux),
- d'autre part, à mettre en place une veille technologique visant à évaluer très régulièrement les nouvelles possibilités cryptographiques afin d'identifier celles qui seraient techniquement et financièrement accessibles.

2.2.4. Obligations anti-blanchiment des PSF de support

La CSSF rappelle aux professionnels financiers disposant d'un statut de PSF de support qu'ils sont également soumis aux obligations d'identification d'opérations suspectes et qu'ils doivent appliquer la législation et la réglementation anti-blanchiment comme tout autre professionnel financier.

Néanmoins, la CSSF est consciente de la spécificité des activités des PSF de support et précise qu'il n'incombe pas à ceux-ci de se substituer à leurs clients, au cas où il s'agit d'autres professionnels financiers, pour réaliser les contrôles à leur place. Si toutefois un employé d'un PSF de support rencontre un cas évident qui relève d'une dénonciation, par exemple s'il identifie le nom d'un terroriste notoire inscrit sur les listes du Parquet, il doit appliquer la procédure de dénonciation prédéfinie établie au sein de son établissement et ne pas informer le client, c'est-à-dire le professionnel financier pour lequel il preste les services.

Les professionnels financiers disposant d'un statut de PSF de support doivent également être attentifs à ne contracter qu'avec des professionnels du secteur financier qui disposent des agréments adéquats et qui font preuve d'une honorabilité certaine. Ceci est particulièrement valable pour les professionnels financiers situés à l'étranger. En ce qui concerne ceux établis au Luxembourg, le PSF de support consultera les tableaux officiels de la CSSF portant sur les établissements agréés au Luxembourg.

De gauche à droite : Constant BACKES (Sécurité des systèmes), Pascale DAMSCHEN (Coordination informatique), Pascal DUCARN (Audit informatique), Marie-Anne VOLTAIRE (Audit interne), David HAGEN (Audit informatique)

Absents : Claude BERNARD (Audit informatique), Geneviève PESCATORE, Marc WEITZEL (Conseillers du Directeur général)

SECRETAIRES DE DIRECTION

De gauche à droite : Monique REISDORFFER, Karin FRANTZ, Marcelle MICHELS

Absente : Joëlle DELOOS