CHAPTER VII

SUPERVISION OF INFORMATION SYSTEMS

1. ACTIVITIES IN 2004

1.1. Meetings, on-site inspections and participation in national groups

In 2004, IT audit participated in 101 meetings and carried out six on-site inspections on subjects covering the functioning and security issues of the supervised entities' IT systems, and more specifically of the entities having a support PFS status, introduced by the law of 2 August 2003 and defined by articles 29-1, 29-2 and 29-3 of the law of 5 April 1993 on the financial sector as amended. A large proportion of these meetings were held with providers of non-financial services that sought information on the authorisation procedure or that were concerned about qualifying their activities in order to determine whether they could be provided without an authorisation.

IT audit has also contributed to seven seminars or conferences and to 38 national meetings held within the framework of working groups or projects. IT audit thus participated, actively or as observer, in some groups of the *Banque centrale du Luxembourg* (Luxembourg Central Bank), the *Comité de Normalisation Luxembourgeois de la Sécurité de l'Information* (CNLSI – Luxembourg standardisation committee of IT security), which contributes to the definition and development of ISO standards in this area, in the design of the training programme of a professional Master in "Management of IT security system" within the University of Luxembourg and in the GRIF research programme which is part of the LIASIT project (Luxembourg International Advanced Studies in Information Technologies), which aims at creating in Luxembourg a centre of excellence in applied research, notably in the field of IT security.

1.2. The GRIF research project

On 30 June 2003, the CSSF signed a co-operation agreement with the *Centre de Recherche Public Henri Tudor* (CRP-HT). The aim of the agreement is to carry out an applied research project, named *Gestion des Risques Informatiques dans le Secteur Financier: nouvelles approches méthodologiques* (GRIF project, IT risk management in the financial sector: new methodological approaches).

This project, which is co-financed by CRP-HT and the CSSF, has been set up in the context of the international harmonisation of banking supervision as defined by the New Basel Accord (Basel II) and more particularly the supervisory mission of the CSSF under Pillar 2, which requires that the supervisory authority reviews and assesses capital adequacy and the internal rating system of credit institutions.

The main objective of the CSSF and CRP-HT consists in studying new methodological approaches allowing to assess IT-related risks, preferably in a quantitative manner. The findings in this highly specific field of research aim to formalise and quantify the consideration of IT risks within the global operational risks of financial institutions.

At year-end 2004, the CSSF and CRP-HT defined a standardised methodology, which does not only apply to IT operational risks, but also to the entire operational risks as defined by Basel II. From this point of view, the project's results surpass initial objectives and are perceived as sufficiently innovating for the CSSF to consider promoting this method to other authorities affected by Pillar 2.

The CSSF and CRP-HT will submit the project's main results to the professionals concerned and to the public by the end of the first half of 2005. The methodology defined within the scope of Pillar 2 can also be used by institutions within Pillar 1. Additional work with the professionals concerned (credit institutions, investment firms, consultants and auditors) is planned to consolidate the method and to promote its understanding by all the other parties involved.

It has to be noted that this method remains compatible with any other method used within the scope of Pillar 1, be it COSO[1], or in the IT area, Cobit, Méhari, EBIOS, etc., and that it presents, by virtue of its standardisation, transparency in the specific assessment of Pillar 2.

1.3. International co-operation

The year 2004 was marked by the end of the works of the Electronic Banking Group (EBG), which will be integrated into another group of the Basel Committee. It has not been defined for the time being which group will take over the EBG's works, but the groups dealing with operational risks are privileged candidates.

The end of the meetings does not imply that there is no communication. The members of EBG regularly inquire about new challenges in the field of international e-banking. The CSSF has thus followed the progression of the "phishing" phenomenon, which has grown rapidly, departing from the United States and Asia, before hitting Europe.

"Phishing[2]" is a form of online fraud, aiming at getting hold, through the Internet, by fraudulent means and by eluding the users, of confidential information that will be used in an unlawful way.

The "phishing" phenomenon proves that data security in the financial world is not only the responsibility and remit of the financial professionals, but that the user of online financial services must also be made aware of the threats and assume his responsibilities in this field. For this reason, the CSSF highly approves the financial institutions that have informed their clients about the existence of "phishing" and the initiatives aiming to inform the public, such as the CASES[3] project.

2. SUPERVISORY PRACTICE

Within the scope of the supervision of operational aspects of support PFS, the IT audit focuses in particular on verifying compliance with the legal and regulatory framework aiming directly or indirectly at maintaining or improving the professionalism of the activities so as to ensure that the quality of the subcontracted services meets the same prudential criteria as the credit institutions that use them.

2.1. Segregation of environments within support PFS

The CSSF stresses that the segregation of client's environments and data by the support PFS is a fundamental element guaranteeing quality and perenniality of activities, notably because it contributes to minimise reputational and, indirectly, legal and financial risks. Indeed, a service provider entrusted with processing the data of several financial institutions must at any time be able to distinguish for which one it is providing a service. He must also be able to ensure perfect impermeability between the entities concerned, so as to guarantee perfect confidentiality of the entrusted data.

[1] COSO Enterprise Risk Management – Integrated Framework. COSO was formed in 1985 to promote the National Commission in the United States, named "National Commission on Fraudulent Financial Reporting" and known as "Treadway Commission" (www.coso.org).

[2] Phishing = (Phreaking + Fishing). Phreaking: hacking telephone exchanges, since the blue Box of John Draper in the seventies. Fishing: reference to password fishing in the Internet ocean.

[3] Cyberworld Awareness Security Enhancement Structure – *Portail de la sécurité de l'information du Ministère de l'Economie* (Portal of data security of the Ministry for economic affairs) (www.cases.lu).

The CSSF reminds that the supervised entities must remain prudent when assessing technical solutions. Thus, IT audit approves or disapproves a solution proposed by an establishment only after having appraised the way the latter has assessed risks, and by balancing this solution against the current good practices and the experience gained with similar cases in the past.

Experience prompts IT audit to be very prudent with respect to solutions for the segregation of environments that are mainly based on procedures, without being supported by technical safeguards. Indeed, the smooth functioning of the procedures implies strict discipline of the persons concerned. Unfortunately, experience shows that this discipline fades with time and as staff changes.

Another aspect of prudence relates to the reliability of the proposed technical solutions in order to guarantee a segregation of environments. The CSSF does not impose one computer to be set up for each financial entity the PFS deals with, which would be contrary to any economy of scale that outsourcing should allow. However, it is advisable to be prudent when a system (computers and other peripheral equipment) is shared by several financial institutions. Resources can be shared in many different ways, but analysis should take into account the reliability of the various operating systems and of the financial applications used. Hence, the CSSF is reluctant to approve the sharing of an application operating on a single system partition, unless this operating mode has been proved over several years. *A fortiori*, sharing of an application by several institutions is unacceptable if each institution connects to a single shared application, as in this case the segregation only depends on the identifier (username and password) used. A user access configuration error or simply the knowledge of another institution's identifier and password (like after change of employer) would permit connection to a third party environment.

Currently, the most commonly used solution in ASP[4] mode remains the multiple partitioning in which an instance of the financial package is operated per user.

The problem is even more complicated in cases of systems that allow a virtual partitioning for multiple operating systems. These solutions are based on products such as VMware and are promising as far as security is concerned, notably when processors will be able to handle the technology of these virtual machines. In this case, one can expect partitioning being done at processor level and not within the operating system of the virtual machine. In these circumstances, the CSSF does not pronounce itself on the reliability of the current solutions and encourages prudence.

2.2. Interim staffing services and the PFS status operators of systems and networks

Several IT service companies contacted the CSSF in order to determine whether their activities fall under the status of IT systems and communication networks operator of the financial sector.

The services of these companies include the provision of specialised staff, namely network engineers, system administrators, or operators specialised in writing operating scripts, to operate production systems or networks of financial institutions.

Last year, the CSSF had already stated its position as regards the status of these services: it considers the administration of a production system as being part of operating a system or a network. *Stricto sensu*, these services thus fall under the PFS status in accordance with article 29-3 of the law of 5 April 1993 on the financial sector as amended.

[4] Application Service Provider, often through the rental at request of a computer application operated by the provider.

However, further clarifications should be added to this position, notably as regards the contractual liability of the subcontractor and the temporary character of the service, to which might be added the purpose of the subcontractor's intervention.

As far as the subcontractor's liability is concerned, the service contract should clearly establish that the subcontractor is only liable for the profile of the persons provided to the company. The contract cannot, by any means, provide for the liability of project finality. The tasks and duties to be carried out by the subcontractor's staff must be entirely defined by the financial institution. Moreover, the provision of services should be limited in time and should not extend beyond the periods allowable for temporary services, in accordance with the existing law in this area, nor be renewed with different staff, which would be considered as offering operator services disguised as temporary services.

The objective of the subcontractor's services is an important element enabling to qualify the activity. Where the services are provided over a reasonable and limited period of time and for non repetitive tasks, such as conversion from one system to another, the activity can be considered as a development project and not as an operating assignment, as the services become void as soon as the migration is complete. In this case, the subcontractor could also be liable for the result of the service and guarantee the project finality, since the provision of the service will not be considered by the CSSF as system operation, but as a specific non-repetitive project.

In order to be able to assess the services on the borderline between those requiring a PFS authorisation as systems and networks operator and those that do not, the CSSF checks in particular if the company concerned fulfils the conditions set out below. It should be noted that the activities on the borderline are those consisting in providing staff specialised in operating functions (systems or networks engineers, operators, production agents, script developers, etc.).

The conditions allowing a subcontractor to qualify its services as temporary work, and not as operating of systems and networks requiring an authorisation as PFS, are the following:

- the provider does not renew services for the same financial institution in a consecutive manner;
- the provider does not assume liability for the finality of the service, which would include the duty to achieve a result, but only for the quality of the profile of the person provided to the financial institution, which entails an obligation of due care;
- the provider lays down by contract that the works and duties to be performed by the staff provided are allocated by the financial institution;
- the provision of the services must *a priori* take place within the financial institution;
- services are provided for a limited period of time in accordance with the law in force in the area of temporary labour.

The CSSF thus endeavours to avoid that the services of systems and networks operators are provided without authorisation and in a disguised manner, in the form notably of systematically renewed temporary contracts.

Furthermore, the CSSF reminds the institutions supervised that sound administrative and accounting organisation rests on the monitoring of the main supporting activities. The financial institutions must therefore avoid to make systematic use of temporary resources for IT functions, in particular relating to production systems and networks.

It is acceptable to replace a computer specialist (i.e. a system administrator), unavailable for reasons of ill-health or any other, by a temporary worker, but the financial institution shall not end up using only temporary workers. Indeed, the systems' sound functioning ensuring the continuity of the financial services offered is only possible if the financial institution keeps the mastery.

Periodic renewal of staff leads, to say the least, to an impoverishment of the knowledge of the production tools, in particular as regards historical knowledge of events and issues encountered. It can also result in a dilution of responsibilities according to the degree of motivation and involvement of temporary staff.

The responsibilities of system administrators in the context of defining the user access rights need also be mentioned, as this activity makes these persons strategic players.

The CSSF therefore requires particular attention from the external auditors in the course of their annual audit.

It is essential that each financial institution ascertains that the subcontracted works comply with the law, as well as with the prudence principles linked to the services of temporary staff mentioned above. A financial institution cannot call upon a subcontractor that does not hold the required license and would be constrained to renounce calling upon this entity. The subcontractor could be prosecuted for illegal exercise of an activity of the financial sector.

2.3 The new telephony technologies: VoIP

The VoIP technology, i.e. "Voice over IP", consists in conveying voice over a network using the IP protocol (the Internet Protocol). Concretely, VoIP is a new telephony mode that allows to use the Internet (public or specific to a company or a group) to communicate.

The use of the VoIP technology by financial professionals raises new supervisory issues, notably as regards data confidentiality. Indeed, with traditional telephony, the internal communications of an institution that has its own telephone exchange remain physically confined within the institution. External communications are transmitted to a telephone company falling under the law on telecommunications that requires it to keep communications secret.

Questions raised by the use of VoIP technology are multiple, such as:

- Is the technology sufficiently mastered so as to ensure that the institution's network equipment is adequately configured and secured? Indeed, ill-configured equipment allows to duplicate the link and listen to the communication with any equipment (VoIP telephone or office computer) connected to the local network.
- Is the network used to convey internal VoIP communications exclusively managed by the Luxembourg institution? If this network, which can be the institution's IT network, is for instance managed by an entity of the group or by the parent company, then principles laid down in circular IML 96/126 will not be fulfilled, as confidentiality will not be ensured.

- If VoIP technology is used to communicate outside the institution, for instance with the other entities of the group, or with the non-VoIP external world, the question arises whether an agreement as networks operator is needed. It is indeed possible that the operator is not a telephony operator in accordance with the telecommunications law. Furthermore, in case of interconnecting IP networks, the company must be protected against intrusions. But firewalls and IDS[5], as far as VoIP is concerned, come up to technological limits and are not sufficiently developed to allow efficient protection. VoIP can thus be used as an intrusion means into a computer network.

These questions are not aimed at discouraging the financial professionals to use VoIP, but show that the implementation of this technology should be carried out cautiously, by correctly analysing the weaknesses and threats. VLAN[6] can be used for local networks segmentation and the implementation of VPN[7] must absolutely be considered in this context.

A prudential approach would consist in apprehending VoIP solutions in the same manner as computer networks. The major risk lies in the implementation of VoIP solutions by certain experts in traditional telephony who are not concurrently specialised in data networks and, above all, are not aware of the CSSF's prudential requirements. A VoIP project shall, under no circumstances, be considered as a simple telephony project.

[5] IDS: Intrusion Detection System. Systems allowing to detect abnormal behaviours (patterns) of a network, which could suppose an intrusion. IDS is like a network anti-virus.

[6] VLAN: Virtual Local Area Network. This technology allows to separate physical networks by allocating a logical security to the transport protocol (Ethernet).

[7] VPN: Virtual Private Network. This technology uses cryptography of transmitted information, ensuring confidentiality between two or several pre-configured participants within the computer network.

First row, left to right:

Marie-Anne VOLTAIRE (Internal audit)

Monique REISDORFFER | Marcelle MICHELS | Joëlle DELOOS | Karin FRANTZ (Executive secretaries)

Pascale DAMSCHEN (IT Coordination)

Second row, left to right:

Pascal DUCARN (IT Audit) | Constant BACKES (Systems Security)

David HAGEN | Claude BERNARD (IT Audit)

Absent:

Geneviève PESCATORE | Marc WEITZEL (Director General’s Advisors)