CHAPTER VII

SUPERVISION OF INFORMATION SYSTEMS

1. Activities in 2003
2. International co-operation

1. Activities in 2003

1.1. Meetings and on-site inspections

In 2003, IT audit participated in 114 meetings and 3 on-site inspections on subjects covering the functioning and security of the supervised entities' IT systems. A little bit more than half of the meetings were held with providers of services, consultants or law firms.

IT audit has also contributed to several seminars or conferences, national meetings held within the framework of projects, such as the setting up of a national certification authority, and to press articles.

As from September 2003, IT audit was greatly solicited by companies seeking information on the legislative changes that took place in August 2003. Indeed, the law of 2 August 2003, amending the law of 5 April 1993 on the financial sector, has, inter alia, introduced three new categories of professionals of the financial sector (PFS) defined under articles 29-1, 29-2 and 29-3 of the law of 5 April 1993, which gave rise to questions falling more particularly under the competence of IT audit. The activities covered by these PFS, considered as connected to the financial sector, do not exclusively rely on the provision of financial services anymore, but on the provision of outsourcing services relating to financial activities. The following statuses are concerned:

- Client communication agents whose services notably include printing of statements of account or confirmations of financial transactions, as well as archiving of documents. As communication can also take place in electronic form, holders of this status are allowed to operate consultative websites.

- Administrative agents allowed to contribute to the business processes of financial institutions and whose services are similar to back office functions.

- IT systems and communication networks operators of the financial sector who intervene on the IT systems of financial institutions, but which are not allowed to intervene within the business lines.

The reader is invited to refer to Chapter I, which provides further information on the specificities of these activities.

With respect to these new activities, IT audit takes account of the concentration risk and verifies the professionalism of the activities, so as to ensure that the quality of the outsourced services meets the same criteria as those required for financial institutions which have recourse to these services.

Particular stress is laid on the segregation of environments and data. Indeed, a service provider entrusted with the work of several financial institutions must at any time be able to distinguish for whom he 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.

Where a company or group creates a new PFS entity and partially transfers staff to this new structure, IT audit verifies that the access rights to premises and systems, which must be reserved to staff of the PFS, are strictly complied with. Indeed, transferring personnel always entails difficulties as regards the management of these changes, in particular where the PFS occupies premises adjacent to those of the company it originates from. It is not always easy or natural for transferred employees to consider their former colleagues, whom they possibly meet every day because of the closeness of the premises, as external parties according to circular IML 96/126. The circular notably defines certain practices that must be complied with as regards access to the production environment and professional secrecy.

Considering the origin of the providers of connected services, who do not necessarily have a "corporate culture" similar to that of an entity subject to the supervision of the CSSF, IT audit intends to insist on the educational aspect rather than on the coercive aspect of supervision. The purpose is to convey the basic mechanisms governing a "sound and prudent" management of the activity to the new PFS. Stress will be laid on the perenniality of the activities, the drawing up of procedures, the four-eye principle, as well as on segregation, integrity and confidentiality of the processed data.

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 the 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 of the supervisory mission of the CSSF under "pillar 2", which requires that the supervisory authority reviews and assesses capital adequacy and the internal rating process of credit institutions.

The main objective of the CSSF and the 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. The knowledge shared is diverse and the project team consists of both CRP-HT researchers and CSSF agents, so as to optimally cover the areas of statistics, mathematics, IT, documentary research, project management, IT systems audit, prudential supervision and systems security and finance.

The GRIF project, in its initial stage, will stretch over two years and consists of four parts. The first part aims to create an "IT and finance" sectorial competence unit, directed towards risk management and IT security. The second part covers the production of a new methodological tool, while the third part consists in validating the results through consultation of local players. The fourth and last part concerns a study on the perpetuation and development of skills, e.g. by widening the partnership with the financial, institutional and IT sectors.

At the end of 2003, the multidisciplinary research team closed the stage consisting in levelling up the participants' knowledge. Thus, each member has a more precise view of the concepts of Basel II, as well as of those of IT risk management. The works on the agenda during the next stage consist in analysing the main components to be taken into consideration as regards IT risk. It is possible that a UML representation (Unified Modeling Language) will allow to better formalise this model: resources used, characteristics of these resources, weaknesses and associated risks, etc. This type of model could lead to a language or formalism shared by institutions which carry out their own risk assessment within the scope of AMA (Advanced Measurement Approach) and by the CSSF, which must validate their approach.

2. International co-operation

IT audit participates in the works of the Electronic Banking Group (EBG) of the Basel Committee. The EBG was instituted in November 1999 with the aim of reflecting on the prudential consequences of electronic banking activities, mainly through the Internet.

The first document entitled "Electronic Banking Group Initiatives and White Papers" has been presented in November 2000 and defined the initiative taken by the Basel Committee on banking supervision.

The document entitled "Risk Management Principles for Electronic Banking" had been drawn up in May 2001 and published in its final version in July 2003. It sets out the main points to comply with in order to ensure adequate risk control as regards e-banking: effective management by the Board of directors and the senior management of the financial institutions, security controls (non-repudiation, authentication, etc.), legal and reputational risk management.

Furthermore, the report "Management and Supervision of Cross-Border Electronic Banking Activities", published for the first time in October 2002, which, on the one hand, identifies the responsibilities of the institutions when setting up a cross-border activity via Internet and, on the other hand, specifies the supervisory modes of the relevant authorities, i.e. the authority responsible for the supervision of the institution offering the service concerned and the authority of the host country in which the service is offered, has been published in its final version in July 2003. This document shows the limits of such a co-operation between authorities, in particular when the home country does not provide for any supervision and the services are provided without any physical presence in a host country requiring that the services provided be supervised.

None of the final versions of these documents has been fundamentally changed. The modifications essentially concern the presentation order of certain footnotes.

During the year 2003, the EBG continued to act as an exchange platform, allowing members to better understand the current challenges as regards e-banking services. These information exchanges, notably in the field of cyber-criminality, show that certain continents, in particular Asia, are subject to a new wave of fake web sites, aiming either to mislead users in order to intercept their identification data on real websites or to intercept credit card numbers, or to illegally collect deposits of the public, whereas the credit institution does not exist. The EBG intends to discuss the subject of the security of electronic financial services in 2004, subject to the approval of the Basel Committee. The stakes represented by outsourcing should also be examined.