CHAPTER VIII

SUPERVISION OF INFORMATION SYSTEMS

1. Activities in 2005

2. Supervisory practice

1. ACTIVITIES IN 2005

1.1. Meetings and participation in national groups

In 2005, IT audit took part in 127 meetings of following categories:

- meetings relating to the scrutiny of applications for authorisation to perform a support PFS activity, in co-operation with the other departments concerned;
- meetings on subjects covering the operation and security of the IT systems of the supervised entities, most of which are granted the PFS status "IT systems and communication networks operators of the financial sector" under article 29-3 of the law of 5 April 1993 on the financial sector as amended;
- meetings with companies that provide services to the financial sector in order to define their activities and determine whether an authorisation is required or not.

These meetings were held with companies offering subcontractor services to the financial sector, IT services companies, law firms, consultancy firms, auditing firms and supervised entities.

IT audit also took part in two international conferences as speaker and attended sixteen seminars or national conferences on subjects relating to IT systems security.

Works related to ISO within the *Comité de Normalisation de la Sécurité de l'Information* (CNLSI – Luxembourg standardisation committee for IT security) have been carried on, as well as those on the design of a professional Master in "Management of IT systems security" (*Management de la Securité des Systèmes d'Informations*, MSSI), in co-operation with the University of Luxembourg and the *Centre de Recherche Public Henri Tudor* (CRP-HT). It should be noted in this context that IT audit participates in two strategic sub-committees set up by CRP-HT to determine the research fields to explore in the areas of Quality and IT systems Security.

1.2. The GRIF research project

The GRIF research project started in 2003 in co-operation with the *Centre de Recherche Public Henri Tudor*. Its purpose is to carry out an applied research project, which was renamed *Gestion des Risques dans les Intitutions Financières* (Risk Management in Financial Institutions)[1] in 2005.

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 which may also cover the entire operational risks as defined by Basel II. Consequently, the project's results exceed the initial objectives and entailed the revision of the project's title in order to reflect the broader scope covered by this model.

[1] The initial title was *Gestion des Risques Informatiques dans le Secteur Financier* (IT Risk Management in the Financial Sector).

The considered model is based on the ISO/IEC 15504 standard, which allows to assess the process maturity. As these processes concern risks, the model could contribute to meeting the new prudential supervisory requirements without imposing constraints on specific procedures, but by promoting the enhancement of the know-how of financial institutions, of their providers (of advice, products and services), as well as of supervisory authorities.

The work achieved within the GRIF project allowed to put forward the advantages of the ISO/IEC 15504 standard, which allows to assess all types of organisations through the maturity of its processes and can thus be implemented by financial institutions to assess the maturity of the operational risk management, as well as of business lines. The undeniable advantage of the ISO/IEC 15504 standard is that it focuses on the expected results (the "what") and not on the way to achieve them (the "how"), which is left at the discretion of the players, but which may nevertheless rely on commonly accepted basic practices that are reflected in assessment questionnaires.

The research done in the context of the GRIF project concerned the establishment of a Process Reference Model (PRM) based on the criteria set down by the New Basel Accord on operational risks. The obtained traceability is bidirectional and allows to validate the origin in Basel II of the processes to assess. The Process Assessment Model (PAM) was developed subsequently, but in order to be able to carry out the assessments, the assessment questionnaires, which should also contain basic practices that should be observed, still need to be drawn up.

The current results of the project, applied within the scope of Pillar 2 of Basel II, would allow the CSSF to obtain an objective assessment of the operational risk management model submitted by the institutions.

At the end of 2005, it appears, following the presentation of the GRIF project to the financial players concerned, that the major appeal of the project is the applicability of the ISO/IEC 15504 standard within the financial sector as assessment and improvement tool for processes, whether they relate to business line or risk management processes. The interested players in the financial sector, as well as CRP-HT and the CSSF, identify several potential application areas for the ISO/IEC 15504 standard within the financial sector. The following list is not exhaustive:

- in the field of outsourcing, in order to assess the aptitude of a provider to deliver its services
  - for the business of investment funds or depositary banks, for example, by developing "business" PRM and associated PAM;
  - for IT businesses, with the AIDA[2] project, which leads to the development of a PRM and a PAM on ITIL[3] , and which would allow to assess the capability of the providers, including the PFS authorised as system operators, to implement ITIL.
- in the field of audit, by establishing a PRM and PAM specific to
  - internal controls;
  - the implementation of IAS accounting standards;
  - the legal requirements, be it the implementation of new functions (e.g. the compliance function), risk management (Pillar 1) or the IT function (circular CSSF 05/178).

The advantage of this method lies in the normative assessment that leads to coherent results and allows, as a consequence, to be carried out by a third party to define the capability level of an institution to manage its processes (or its operational risks in the context of Basel II) in a repeatable manner.

[2] Assessment and Improvement Integrated Approach", CRP Henri Tudor project (www.crpht.lu).

[3] IT Information Library (ITIL) is a set of good practice used to deliver high quality IT services.

It is also possible to carry out a self-assessment by or on behalf of an institution to define the relevance of its own processes and to improve them, for a particular purpose or for a whole set of requirements (Pillar 1 of Basel II).

The full documentation on the GRIF project is available on the CSSF website (www.cssf.lu) under the heading "Info kits", sub-heading "Capital adequacy", section "GRIF project: Operational risk management in financial institutions".

1.3. International co-operation

IT audit took part in the annual International Supervisory Group on IT conference, which gathers the persons responsible for the prudential supervision of the IT systems of the different authorities[4]. The aim of this group is to promote the exchange of information relating to the current technological stakes and covers aspects such as business continuity plans, electronic banking, countermeasures against the phishing[5] phenomenon and the supervision of cross-border IT outsourcing. Throughout the year, the group's members exchange information concerning frauds related to IT and Internet, attacks against information systems, identity theft or weaknesses of certain systems.

2. SUPERVISORY PRACTICE

Supervision covers verification that the supervised entities implement the legal and regulatory framework, with the direct or indirect purpose to maintain or improve the professionalism of the activities, focusing in particular on aspects related to implemented technologies as regards information systems and taking account of the specificities of the support PFS, which offer their subcontracting services to the other supervised institutions.

2.1. Reminder of the fundamental prudential considerations

As far as the supervision of support PFS is concerned, the CSSF invites the reader to refer to Chapter VII, point 2.1 of the CSSF's Annual Report 2004, which underlines the importance of segregation of environments and customer data (the financial professionals). Indeed, IT audit considers that it is crucial for a support PFS to guarantee impermeability between environments, irrespective of the technological options set up to mutualise resources. Moreover, the prudential principle of segregation of functions, which improves controls, allows to reduce errors or frauds and is widely implemented by financial professionals, shall also be implemented by providers, whether they are authorised as support PFS or not. IT audit insists on the importance that this prudential principle is applied within support PFS and, in particular, IT systems and communication networks operators of the financial sector.

The CSSF also observed a relatively large cultural gap between certain support PFS, authorised as client communication agent or IT systems and communication networks operator of the financial sector, and the financial professionals they serve. This cultural difference is expressed by an often insufficient understanding of ethical rules pertaining to the financial sector and, in particular, by a commercial use, or even advertising use, made of the ministerial authorisation. Yet, the wording of article 52(3) of the law of 5 April 1993 on the financial sector as amended leaves no room for doubt: "No person shall make use for commercial purposes of his registration on an official list or of the fact of his being subject to supervision by the CSSF".

[4] The group was initially named "HITS" (Head of IT Supervision). The authorities of the following countries were present: United States, France, Belgium, the Netherlands, Luxembourg, Italy, Spain, Singapore, Hong Kong, Australia, Canada, Germany, Norway and Great Britain (Sweden and Switzerland were absent in 2005).

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

It appears that many support PFS wrongly assume that the authorisation and the associated supervision are equivalent to a certification or quality label. The major consequence of an authorisation is however that it imposes the same legal and regulatory framework as the one applicable to financial professionals. It is a legal obligation in order to be authorised to exercise this activity and not a voluntary recognition. Bringing out the ministerial authorisation too visibly and commercially *vis-à-vis* financial professionals, which are potential customers, can have the opposite effect as that pursued, if the ethical divide observed by the CSSF is thereby revealed.

2.2. Clarifications of certain questions put to the CSSF

2.2.1. Remote accesses: use by a supervised entity of the mobile messaging "push-mail" and the "BlackBerry" product

A "push-mail" solution is based on a messaging infrastructure that involves one or several mobile network operators to convey electronic messages from the company's internal messaging system to a mobile equipment, and vice-versa. This type of messaging relies on the principle of proactivity of the mobile equipment, which queries the messaging server very regularly in order to retrieve any messages awaiting transfer. Everything takes places as if the server would contact the mobile equipment when messages are queued, hence the term "push-mail". Mobile equipment shall thus be able to operate specific "push-mail" programmes. This is the reason why such equipments are currently mobile phones with a sophisticated operating system (such as Symbian) or PDAs[6] with mobile phone functionalities, which communicate through a GPRS or UMTS connection of GSM network operators.

In order to define the security criteria to be fulfilled in order to be allowed to use a push-mail solution, it is necessary to qualify the information that will transit from the professional of the financial sector to the mobile equipment. This information is, *a priori*, considered by the CSSF as confidential, as it stems from the internal messaging system of the company and contains inevitably references to customers at one point or another. Consequently, the solution must ensure confidentiality and, preferably, the integrity of the information exchanged between the push-mail server and the mobile equipment.

The push-mail server shall therefore be under the exclusive control of the professional of the financial sector and be located on its premises in Luxembourg.

The unavoidable use of mobile operators also imposes the encryption of the exchanged data.

The mobile user shall also be identified by the server in order to ensure that the latter is really entitled to read the confidential data. The sole use of the PIN code of the SIM[7] card cannot suffice, in particular if the unentitled user replaces the original SIM card by a card of which he knows the PIN code. The solution should thus provide for a specific PIN code or be linked to the SIM card of the entitled user.

Finally, if the mobile equipment is lost or stolen, the data it contains shall not be legible by a third party and shall therefore be strongly encrypted and, preferably, remotely deletable.

The most commonly known push-mail solution has been designed by the British company Research In Motion Ltd (RIM) and is called BlackBerry®.

Many entities under the supervision of the CSSF enquired about the possibilities or restrictions as regards the use of the BlackBerry® solution.

[6] PDA: Personal Digital Assistant (palmtop computer, running the operating system Palm OS or WindowsCE and derivatives).

[7] Chip card provided by the mobile operator.

Since the mobile equipment and the server are provided by RIM, knowing that all messages pass through a platform of RIM in the United Kingdom, and unless the said company provides high-level third-party certifications proving the security measures it sets forth and the impossibility for third parties, including itself, to decode the transmitted data, the CSSF advises to be prudent with respect to this solution. Nevertheless, the trust placed in RIM is being checked by certain States, such as the United States of America and France, which use this solution at the highest State and corporate level. Certifications should thus be available soon. The professionals of the financial sector will be responsible for verifying the coverage thereof and for determining the trust to be placed in this solution.

Certain implementation rules should however be complied with. On the one hand, the professional of the financial sector shall at least use the option proposed by RIM, which consists in allowing the professional of the financial sector to manage the cryptography keys itself, and on the other hand, the professional shall dispose of the function of remote deleting of the messages stored on the lost or stolen mobile equipment.

As long as the professionals of the financial sector manage their BlackBerry® infrastructure themselves, this solution should not be considered as outsourcing and a prior approval by the CSSF is not required.

2.2.2. Monitoring services performed by a provider without support PFS status

The CSSF confirms that monitoring services, whether they consist in overseeing applications, IT systems or networks, are not considered as operating services and are not subject to an authorisation if the service provider is not able to intervene on the monitored equipment.

The essential condition for the provision of such services without authorisation is to impose in the contract and operationally that the provider's customer is to carry out the necessary corrective intervention. In this case, the professional of the financial sector decides on the actions to be taken following the monitoring and shall oversee the actions of the provider in accordance with the indications given in circular CSSF 05/178.

2.2.3. Cryptography of very high bandwitdh lines relying on fibre optics

The development of telecommunications allows to use very high bandwidth transmission lines that rely on fibre optics and that enable the connections of central units at processors level so as to make remote "multi-processing" possible. Thus, the workload of the central processing units can be divided over distances of several kilometres, thereby ensuring a redundancy of equipment in the event of a disaster on one of them.

The main drawback of these technologies is that cryptography of these high bandwidth highways becomes very costly, even prohibitive, while the CSSF requires that the communication between the professional of the financial sector and the remote processing centre is protected.

Where it is technically impossible, or disproportionately costly, to encrypt the line or data, the professional of the financial sector shall nevertheless ensure that no third party, and in particular, no access provider to telecommunication lines not legally bound by the communication secrecy, has non-controlled access to the data that pass through this line. The specificities of fibre optics however allow to envisage a control of the line's integrity, which would rely on the identification and justification by all providers involved in the supply of this line, of any communication breakdown. Indeed, it is highly unlikely for a third party to connect to or to track the content of the data exchanged on this type of line without having to physically intervene on the network and to provoke in this case a temporary failure of the fibre optics.

Nevertheless, the CSSF invites the professionals of the financial sector:

- on the one hand, to envisage solutions that provide for a prior encryption of each service, according to the criticality of the exchanged data, which amounts to not encrypting the whole line, but only the different flows that concentrate on the line (logic multiplexing of flows);
- on the other hand, to set up a technology watch aiming to assess on a regular basis the new cryptographic possibilities, in order to identify those that would be technically and financially accessible.

2.2.4. Anti-money laundering obligations of the support PFS

The CSSF reminds the financial professional that have a support PFS status that they are also subject to the obligation to identify suspicious transactions, and that they shall apply the anti-money laundering laws and regulations as any other professional of the financial sector.

Nevertheless, the CSSF is aware of the specificities of the support PFS' activities and specifies that they are not required to substitute for their customers, in case they are other professionals of the financial sector, to carry out the controls instead of them. However, if an employee of the support PFS becomes aware of an obvious fact that should be reported, for example, if he identifies the name of a notorious terrorist included in the list of the Public Prosecutor's office, he shall apply the predefined reporting procedure set up within its institution and refrain from informing the customer, i.e. the professional of the financial sector to which he provides his services.

The financial professionals authorised as support PFS shall also ensure that they only contract with professionals of the financial sector that have been granted the appropriate authorisation and prove that they have a sound professional repute. This is particularly true for the financial professionals located abroad. As far as those established in Luxembourg are concerned, the support PFS shall look up the CSSF's official lists of institutions authorised in Luxembourg.

Left to right: Constant BACKES (Systems Security), Pascale DAMSCHEN (IT Coordination),
Pascal DUCARN (IT Audit), Marie-Anne VOLTAIRE (Internal Audit), David HAGEN (IT Audit)
Absent: Claude BERNARD (IT Audit), Geneviève PESCATORE, Marc WEITZEL (Director General's advisors)

EXECUTIVE SECRETARIES

Left to right: Monique REISDORFFER, Karin FRANTZ, Marcelle MICHELS
Absent : Joëlle DELOOS