CHAPTER

VI

SUPERVISION OF INFORMATION SYSTEMS

The principal mission of the CSSF information technology (IT) audit is the prudential supervision of information systems, i.e. consideration of technological aspects relating mainly to data processing and telecommunications in supervising the financial sector. Rather than financial risks, the information technology audit examines the operational risks arising when financial institutions use information technology systems. In order to assess operational risks, the information technology audit often bases the examination of projects submitted to the CSSF or on-site inspections on a comparative assessment of good practice in information technology.

1. Activities in 2002

1.1. Meetings and on-site inspections

In 2002, the IT audit held meetings and carried out on-site inspections covering the functioning and the security of IT systems of the supervised entities. The letters addressed to the supervised establishments mainly concerned specific observations relating to the submitted projects or were sent in response to comments made by external auditors in their specific or annual reports.

The principal activities covered by meetings and on-site inspections are the same as last year, but in different proportions:

- Internet websites remain topical, in spite of generally less ambitious activities or projects in this field. The new websites are more oriented towards secured mail services and the verification by clients of their assets than towards the possibility of real-time order placement.

- Outsourcing IT activities is growing and aims to cut costs by sharing the necessary resources and to improve services thanks to specialised personnel in the outsourced activity.

- In 2002, relocation of systems at parent companies was quite similar to the outsourcing activity as the objective consists in optimising skills present within the group as regards the exploitation of systems.

- Defining business continuity plans and IT backup solutions is a recurring and stable subject compared to 2001, with questions emerging concerning the impact on operational risks and their assessment in the context of the New Basel Accord.

- Remote access to the IT platform by certain employees from their home is an emerging question put to the CSSF. It is supported with arguments concerning cost-cutting while preserving the specialisation of system administrators in charge of intervening (availability and transport costs). Security is the main critical element that needs to be examined in more detail.

IT audit is regularly approached by IT companies and consultancy firms in charge of developing projects for clients of the financial sector. The dialogue initiated in 2001 took concrete form with 21 meetings held in 2002.

It must be stressed, as in the past, that the CSSF does not approve companies which are not under its authority and in no way awards a specific conformity label to the services provided by the companies, which do not receive any form of a certification following such meetings.

1.2. Survey on continuity plans

In 2002, the CSSF conducted a survey on Business Continuity Plans (BCP), following the numerous questions raised in this field since September 2001. Before making any recommendations, the CSSF took stock of the situation, resulting in the publication of the document "Survey on BCPs as at 31 August 2002" sent to all the credit institutions and other professionals of the financial sector under its supervision.

The examination of the results is being finalised, but certain characteristics, based on a sample of 71 credit institutions of various size and 43 professionals of the financial sector (PFS) have already been identified.

- Large and medium-sized institutions generally defined a BCP covering all the activities, supported by an important redundancy of IT systems and specific premises to be used in case of disaster.

- Small-sized institutions, among which a large number of PFS, mix up BCP and backup, i.e. they plan to pursue their activities mainly thanks to an IT backup centre. This conception is in fact equivalent to the notion of Disaster Recovery Plan (DRP) encompassing the means of implementation of a BCP. This kind of approach may prove incomplete if the BCP does not take account of the whole resources necessary for their activities, i.e. at least the personnel and the business premises.

- At present, a high number of medium and small-sized institutions do not have a BCP, but have initiated a project.

- Medium and small-sized institutions have massively recourse to specialised providers of IT backup infrastructures. There are only a few providers of shared backup centres, and, as a result, despite the fact that they allow to set up backup solutions at lower costs, they represent a relatively high risk of concentration in case of disaster to affect several financial institutions. This risk also depends on the different categories of contracts and their geographical distribution in relation to the place of disaster. The signatory institution of the "weakest" contract is more at risk than the others.

In some countries, authorities became normative and imposed minimal distances between two processing centres of a financial institution. The CSSF does not yet consider defining such a criterion, owing in particular to the small dimensions of the Grand Duchy and the typology of its communications infrastructure, which shows a small number of strategic hubs, which are less than twenty kilometres apart.

1.3. Other important events

The intention to subcontract certain activities was certainly the most important trend in 2002. The CSSF was approached concerning three categories of outsourcing activities at the parent company or an entity of the group subject to the supervision of the home authority:

- Consultative Internet websites;

- SWIFT access within the scope of SWIFTNet migration;

- Management of the Active Directory Service within Microsoft Windows 2000.

IML Circular 96/126 specifies that confidential pieces of information cannot be relocated outside Luxembourg, in particular if they are available to third parties. A case-by-case analysis by the CSSF reveals the following trends:

a) Consultative Internet websites

Given the high cost of security infrastructures needed to protect networks connected to the Internet, certain medium and small-sized institutions wished to use the sizeable infrastructures of their parent company to be able to offer consultative services to their clients.

When no information transmitted to the parent company allows to identify the client, i.e. when statements of account do not contain any information other than the anonymous identifier, and considering that the planned infrastructure and organisation are state of the art[1], the CSSF allowed recourse to outsourcing on an ad hoc basis, in accordance with the conditions laid down in IML Circular 96/126. The CSSF also requested the institutions concerned to provide a confirmation from the supervisory authorities of the country were the outsourcing activity takes place, approving the IT connection and confirming that security standards in use are appropriate.

b) SWIFT access within the scope of SWIFTNet migration

The objective of the SWIFT network, the use of which is restricted to professionals of the financial sector throughout the world, consists in the transmission of secured and authentic orders (delivery guaranteed) between its members. This network is the primary means of communication between financial institutions all over the world.

The Swift company decided to develop its network by adopting the most widely used standard: the Internet-specific IP protocol. This development enables members to use more widespread and easily inter-operating equipment. The migration also provides for the use of the electronic signature based on a public key infrastructure (PKI) and the modification of the message formats with the adoption of the ISO 15022 standard, a variation on the XML model. The new network is called SWIFTNet.

The CSSF was confronted with requests from credit institutions established in Luxembourg wishing to use an access platform to SWIFTNet located at their parent company. These institutions argued that the high costs of the migration towards SWIFTNet would penalise their activities in Luxembourg; the suggested alternative consisted in sharing the SWIFTNet infrastructure.

The CSSF considers that the implementation of a common relocated infrastructure calls for a more thorough study.

The use of a common relocated infrastructure of a provider outside Luxembourg, at the parent company or at a company offering “office services”, presupposes the transmission of the SWIFT message from the Luxembourg establishment to the SWIFT access point located outside the Luxembourg territory. Technically, these data, which contain the name of the originator, are temporarily available on the SWIFT station, despite the fact that they are encrypted during their transit, before they are encrypted and sent through the SWIFT network. Presently, an inadequate programming of the SWIFT station may entail a more or less long-lasting storage on the station, breaching the provisions of IML Circular 96/126.

[1] *See also the CSSF report “Services financiers par Internet” of 2001.*

With SWIFTNet, a distinction has to be made between the SWIFT station, on which messages are drawn up, and the access point, called gateway, which concentrates the sent messages in the network. The way the station and the gateway are connected depends on the establishment and not on SWIFT. If the gateway is located at a subcontractor or the parent company, the message will transit for a moment in decoded form through the gateway. The Luxemburg establishment must then ensure that no tool or individual – i.e. a system administrator or other – is able to intercept these messages.

Consequently, relocating a SWIFT platform entails a risk of disclosing confidential information. The CSSF will examine solutions so as to prevent this risk.

The *Association Luxembourgeoise des Membres et Utilisateurs SWIFT* (ALMUS) examines the setting up of an "office service" in Luxembourg, consisting in a local alternative of sharing a SWIFTNet access platform so that the Luxembourg financial community would dispose, within the time limit set by SWIFT to implement the migration towards SWIFTNet, of a local alternative to share IT resources, insofar as one or several service providers would offer such activities.

c) Management of the Active Directory Service within Microsoft Windows 2000

Users of the Microsoft Windows 2000 operating system dispose of a resource (mainly user directories) management mechanism, called Active Directory Service (ADS), which allows to centrally manage access rights of the users connected to the network. The distinctive feature of the ADS lies in the possibility to administer several networks of a single geographical or logical business unit from an arborescence.

Some Luxembourg establishments, belonging to international groups, which installed Windows 2000 in all their entities with the purpose of a uniform and simplified management of IT resources, asked the CSSF whether the ADS could be administered by the parent company.

Given that the main administrator of the ADS, who disposes of the "root" function, is able to create and modify the access right of any user defined in an arborescence, he is also potentially able to access any available resource defined therein. Considering that the local network of a financial establishment is likely to contain highly confidential data (letters to clients, strategic recommendations, contracts, etc.) stored in one or several files or internal electronic mail servers, it is most important that this establishment has full control over the access rights to its resources. If a third party system administrator, relocated out of the Luxembourg establishment, is in charge of the ADS management and has the possibility to bypass existing security mechanisms and gain access to confidential resources, the centralised administration will not be approved.

The CSSF stresses that further to the obligations relating to professional secrecy, financial institutions have to control all their activities, including outsourced activities. Security aspects conditioning the use of IT resources must be overseen by the financial institution.

2. International co-operation

The IT audit participates in the Electronic Banking Group of the Basel Committee (EBG). The EBG was created in November 1999 with the aim of considering the prudential consequences of electronic banking activities, especially those arising through the use of the Internet.

The first document, "Electronic Banking Group Initiatives and White Papers", was published in November 2000 and defined the initiative taken by the Basel Committee on Banking Supervision.

In May 2001, the EBG issued the conclusions concerning the risks associated with banking services provided through Internet. The document "Risk Management Principles for Electronic Banking" sets out the main points to comply with in order to ensure adequate risk management for electronic banking: effective management by the Board of directors and senior management of financial institutions, security checks (non repudiation, authentication, etc.) and legal and reputational risk management.

Following the publication of these documents, the EBG decided to focus on cross-border aspects of the Internet banking activities. In October 2002, the EBG published the "Management and Supervision of Cross-Border Electronic Banking Activities" report, which, on the one hand, identifies the responsibilities of the institutions when implementing an electronic cross-border activity and, on the other hand, specifies the supervisory modes by the relevant authorities, i.e. the authority in charge of supervising the institution providing the service and the authority of the host country in which the service is provided. The document indicates the limits of such a co-operation between authorities, in particular when the home country does not provide for any supervision and the provision of services takes place without any physical presence in the host country, which requires that the provided service be supervised.