In case of discrepancies between the French and the English text, the French text shall prevail.

Luxembourg, 11 April 1996

To all credit institutions and other professionals of the financial sector[1]

CIRCULAR IML 96/126

Re: Administrative and accounting organisation

Ladies and gentlemen,

The purpose of this circular is to clarify the application of Article 5(2) of the law of 5 April 1993 on the financial sector for banks and Article 17(2) of the same law for the other professionals of the financial sector (hereinafter referred to as PFS).

This circular specifies particularly the security measures which banks and PFS shall take as regards the IT organisation in order to meet the bank secrecy requirements which apply to them.

1. Content of Articles 5(2) and 17(2)

Articles 5(2) and 17(2) provide that banks and PFS authorised to carry out their activities in Luxembourg shall have a sound administrative and accounting organisation. This circular aims to define its requirements.

This circular cannot claim to contain comprehensive rules given the diversity and complexity of the transactions undertaken by banks and PFS, but it rather aims to provide general guidelines governing the design and operation of the administrative

[1] Circular IML 96/126 no longer applies to credit institutions and investment firms. For these entities, the circular has been replaced by Circular CSSF 12/552, as amended.

and accounting organisation. The organisational requirements with respect to specific areas of the activities of a bank or a PFS are set out in specific circulars such as Circulars IML 93/101, IML 93/102 and IML 95/119 relating to the internal organisation and control of the market activity and of derivative activities.

This Circular should be read in conjunction with Circular IML 95/120 on central administration. Indeed, the requirements of the latter circular are fully met only when organisation quality standards as defined in this circular are achieved.

The rules defined hereinafter are, where appropriate, to be adapted to the size and nature of the activities of an institution. This is, for example, the case for certain categories of PFS which carry out specialised activities.

2. Scope

Articles 5(2) and 17(2) of the aforementioned law are applicable to banks and PFS, respectively, which are legal persons governed by Luxembourg law, including their branches abroad.

Credit institutions governed by Luxembourg law shall ensure that the rules defined hereinafter are applied by their subsidiaries established in Luxembourg and transposed by their subsidiaries abroad, insofar as the subsidiaries fall within the scope of the consolidated control exercised by the IML.

As regards the branches in Luxembourg of banks having their registered office outside the EC as well as branches of PFS of EC origin or not, Article 35(4) of the aforementioned law provides that they are required to produce evidence of the existence of a satisfactory administrative infrastructure in Luxembourg. In order to meet the requirements of the law, the rules defined hereinafter are applicable to these branches.

As regards the branches in Luxembourg of banks having their registered office in another EC Member State, the IML specifies in Circular IML 93/100 the requirements on the administrative infrastructure which are specifically applicable to them. In order to meet the bank secrecy requirements which are applicable to them, branches shall, in principle, comply with the rules provided for below as regards the organisation of the IT function. However, as regards the branches belonging to banks or PFS which also have a subsidiary in Luxembourg, they are allowed to use the IT system of the subsidiary provided that the conditions laid down under item 4.5.2.1. and item 4.5.2.2. (except for condition (e)) below are complied with. In particular,

neither the personnel of the subsidiary nor third party specialists in IT consulting, programming, maintenance or management that the subsidiary can use, where appropriate (cf. item 4.5.2.1. hereinafter) may have access to the confidential data of the relevant branches. Inversely, the personnel of the branches concerned cannot have access to the confidential data of the targeted subsidiary.

3. Responsibility of the institution's management

The persons in charge of the daily management and authorised pursuant to Articles 7(2) and 19(2) of the law on the financial sector (hereinafter referred to as "the management") are responsible for the establishment of a sound administrative and accounting organisation. This organisation reflects the powers of the management and the delegation made in this regard, under its responsibility.

By establishing a sound administrative and accounting organisation, the management pursues, in particular, the following objectives:

- ensuring the sound administration of securities and assets;

- ensuring the adequate execution of transactions;

- ensuring the correct and comprehensive registration of transactions and the provision of reliable and quickly available information;

- ensuring the implementation of the decisions taken by it or by the persons acting by delegation and under its responsibility as well as the compliance with the rules imposed during the exercise of the bank or PSF activities.

The management lays down in writing the rules of a sound administrative and accounting organisation. It determines the human and technical means to be implemented. The principles and rules of organisation relate to all the operational, administrative and accounting areas of functioning of the bank or the PFS.

The management ensures that an organisation manual is established. It shall include at least a set of procedures on the administrative organisation (cf. item 4.2.), accounting procedures (cf. item 4.5.1.) as well as a definition of the functions and responsibilities related thereto (cf. item 4.1.). The level of detail of this manual depend on the type of activity and the complexity of the organisational structure.

The management designates one of its members to be in charge of the administrative and accounting organisation and who shall assume responsibility for implementing the policy and rules that it has established in this context. S/he is, in particular, responsible for the establishment of this organisation manual which s/he shall submit to the management for approval prior to its implementation. S/he shall then ensure its proper implementation.

The institution may provide that the definition and the follow-up of the procedures as regards a specific area of activity are the responsibility of the member of the management in charge of this activity, as provided for in Circulars IML 93/101, IML 93/102 and IML 95/119. In this case, the member in charge of the administrative and accounting organisation ensures a consistent and coordinated approach in the institution and the implementation of these procedures in all areas of activities.

As may be inferred from item 4.5.1. below, the member in question shall also be in charge of the provision and publication of accounting information intended for third parties and the transmission of periodic information to the IML. Thus, s/he shall ensure that the form and content of this information comply with the legal and IML rules in this field.
The mode of operating of the management may provide that the responsibilities in the area of administrative organisation and those in the accounting area are shared by two people who are members of the management.

Prior to 30 September 1996, banks and PFS shall indicate the name(s) of the person(s) designated to the IML; any change shall be mentioned by the management to the IML and the long-form report is to be drawn up by the statutory auditor shall include such a change (cf. item 5 in this regard).

4. <u>Sound administrative and accounting organisation</u>

Each bank and each PFS shall have an administrative and accounting organisation complying with the conditions defined hereafter, which relate, in particular, to:

- operating staff;
- execution venues;
- documents relating to transactions;
- administrative infrastructure of the business functions;
- support functions.

In each area, the organisation to be implemented shall be adequate to the principle of effective internal control.

The detailed requirements to be complied with as regards the internal control procedures will be the subject of a specific circular.

4.1. Operating staff

The institution shall have a sufficient number of competent persons on-site in order to take decisions under the policies laid down by the delegated powers, and in order to implement the decisions taken. These tasks are carried out on the basis of a detailed description set by the management and within the framework of an organisation chart of functions adopted by it.

The organisation chart includes for the different departments their structure and their reporting and business lines between them and with the management.

The task description to be filled in by the operating staff shall explain the function, powers and responsibility of each officer.

The organisation chart and task description shall be established based on the principle of segregation of duties. Pursuant to this principle, the duties and responsibilities shall be assigned so as to avoid that they are incompatible for the same person who is not a member of the management, regardless of his/her position in the hierarchy. The goal pursued is to prevent, through a peer review environment, a person from making mistakes and irregularities which would not be identified.

Where, due to the small size of the institution, several duties and responsibilities have to be assigned to the same person, this grouping shall be organised so that it does not prejudice the objective pursued by the segregation of duties.

The organisation chart and task description shall be laid down in writing and made available to all relevant staff. They may usefully be part of the organisation manual (cf. item 3. above).

4.2. Execution venues

4.2.1. The institution shall develop procedures for the execution of transactions. These procedures shall be established in writing as provided for in item 3

above. In order to ensure that the procedures are effectively followed, the necessary controls are to be planned.

The description of the procedures relates to the following points considering the complexity of the institution:

- successive and logical stages of the transaction processing, from initiation to documentation storage;
- flow of the documents used;
- periodic reviews to be carried out, as well as the means to ensure that they have been carried out.

As the purpose is to ensure that the transactions are properly executed, the procedures' content should be clear and comprehensive and made known to all employees concerned. Moreover, the procedures shall be updated forthwith when an internal or external change having an impact on their content takes place.

4.2.2. The institution shall also have the technical equipment required for the execution of its transactions. In this regard, the principles laid down as regards the IT tool as support function shall apply (cf. 4.5.2. below).

By way of illustration, an institution which processes market transactions shall have its own front office and back-office organised in accordance with the rules laid down in Circulars IML 93/101 and 93/102.

4.2.3. All transaction orders initiated by the bank and all contracts with the customers or their proxies shall be issued by the institution in Luxembourg; all correspondence shall be addressed to and send from the institution. In the case where the institution has a branch abroad, the latter is the contact point for its own customers.

4.3. <u>Documents relating to transactions</u>

Any process which includes a commitment on the part of the institution as well as the decisions relating thereto shall be documented. The documentation shall be updated and kept by the institution in accordance with the law. It should be organised in such a way that it can be easily accessed by any authorised third party.

By way of illustration as regards credit transactions, full documentation of the decisions to grant, change or terminate loans shall be included in the institution's files in Luxembourg, as well as the agreements and any documents relating to the follow-up of the debt service and evolution of the debtor's financial situation.

4.4. Administrative infrastructure of the business functions

Each business function shall be based on an adequate administrative infrastructure. This infrastructure shall guarantee the implementation of the business decisions taken and their proper execution, as well as the compliance with the powers and procedures for the area in question.

4.5. Support functions

The accounting and IT functions require the following additional clarification:

4.5.1. Accounting function

4.5.1.1. The accounting organisation implies that the institution shall have a financial and accounting department whose mission is to assume the accounting management of the institution. Some parts of the accounting function within the institution may be decentralised, provided however that the central accounting department centralises and controls all the entries made by the various departments and prepares the global accounts. The accounting department shall ensure that other departments intervene in full compliance with the chart of accounts and the instructions relating thereto. The central department shall remain responsible for the preparation of the annual accounts and the preparation of the periodic information to be provided to the CSSF.

The accounting management shall operate according to the rules and procedures which allow:

- identifying and recording all transactions undertaken by the institution;
- explaining the changes in the accounting balances from one closing date to the next by keeping the movements which had an impact on the accounting items;
- preparing the accounts by applying all the valuation and accounting rules laid down by the accounting laws and relevant IML regulations;

- issuing periodic information and providing supervisory authority with it;

- keeping all accounting documents in accordance with the applicable legal provisions;

- drawing up, where appropriate, accounts according to the accounting scheme applicable in the home country of the shareholder in order to prepare consolidated accounts;

- issuing reliable financial information quickly available to the management ("management information") in order to enable it to closely monitor the developments in the financial situation of the institution and its compliance with budget data. This information shall be used as management control tool and will be more effective if it is based on analytical accounting.

Larger-sized institutions should have a management control which is attached either to the accounting management or, in the organisation chart, directly to the management of the institution.

The tasks carried out within the accounting department cannot be combined with other incompatible business and administrative tasks.

4.5.1.2. In connection with opening counterparties' accounts, each institution shall define specific rules on the recording of accounts in its accounting system. Moreover, it shall specify the conditions under which the authorisation is granted so that these accounts work and under which conditions they might be closed.

The institution shall avoid having, in its accounting records, a multitude of accounts with uncontrollable items that could lead to the execution of non-authorised or fraudulent transactions; particular attention should be paid to dormant accounts. In this respect, the institution shall put in place appropriate verification and monitoring procedures.

4.5.1.3. The opening and closing of internal accounts in the accounting records shall be validated by the accounting department before these accounts become operational. The institution shall set out rules concerning the use of such accounts and the powers relating to their opening. The accounting

department shall ensure that the internal accounts are periodically subject to a justification procedure.

It is necessary to ensure that internal accounts and payable-through accounts which would no longer be suitable for a use defined by the rules are not kept open.

4.5.1.4. The entire accounting organisation and procedures are described in an accounting procedure manual or book, as provided for in item 3 above.

4.5.2. IT function*

Financial professionals shall organise their IT function in order to control it, to ensure its quality and to guarantee the strict protection of confidential data entrusted to them by their clients.

4.5.2.1. - These requirements are best fulfilled when the IT function of the financial professional is performed by its own, well organised, IT department supervised by an internal control framework established by the board. Generally, the financial professional must have, in premises at its disposal in Luxembourg, its own computers and adequate and duly documented IT programmes and hire competent personnel to manage its IT system. Moreover, the financial professional shall be in a position to ensure normal operations in case of an IT-system outage and shall put in place a backup solution in line with a business continuity plan. The business continuity plan aims at describing the actions to put in place in order to continue the activities in case of an incident or disaster linked to unusual events.

- Financial professionals with their own computer system may rely on third party for the provision of advisory, programming and system maintenance services. System operation and management services, however, fall under the status of IT systems and communication networks operator of the financial sector (art. 29-3 of the Law). Financial professionals may thus only rely on financial professionals authorised in accordance with article 29-3 of the Law for the provision of IT managed services or, provided that these systems do not include any readable confidential data, on a supervised entity of the group (cf. 4.5.2.2.) or on an entity of the group benefiting from the exception provided under article 13(2). A third party

* Please also refer to Circular CSSF 05/178 which amends this item.

providing advisory, programming or system maintenance services may be a specialised company in IT owned or not by the financial professional, a company specialised in IT created jointly with other financial professionals (banks or PFS), which cooperate in IT matters, or also a support PFS. The financial professionals concerned may however not evade their liability to maintain secret the information which is entrusted to them, except towards a support PFS, in the relation of the service level agreement falling under the tasks entrusted.

Financial professionals are exposed to a higher disclosure risk when resorting to providers other than support PFS for such services than if they were using their own staff to manage their IT system.

Considering this risk, it is important for financial professionals relying on third parties to comply with the following conditions:

(a) Any outsourcing shall be formalised by a service level agreement including the requirement specifications taking into account the conditions below.

(b) Outsourcing IT services shall not result in transferring the accounting function, including data inputing, to this third party.

(c) In order to allow financial professionals to evaluate whether the data produced by the IT system is reliable, comprehensive, and in line with the accounting and internal control principles, it shall:

- Ensure that any intervention of a third party other than a support PFS, in particular any modification brought to the programmes, is subjected to a prior consent.
- Have among its staff a person with the necessary IT knowledge to understand both the effects of the programmes on the accounting system and the actions undertaken by the third party in the context of the service provided.
- Have in its premises sufficient documentation on the programmes used.

(d) The financial professional shall ensure that there are, if needed, no legal obstacles to obtain the access to operating systems which have been developed by this third party. This is achieved, for example, when the financial professional is the legal owner of the programmes. The financial professional shall anticipate the actions to take in order to

ensure the continuity of the services provision in case the third party defaults.

(e) For protection and confidentiality reasons, third parties other than support PFS cannot be granted access to confidential data.

(f) The prohibition to access confidential data also applies to third parties other than support PFS in charge of the IT system maintenance and management in the case of an entity owned by the group. If access to some data cannot be avoided when fixing a major system disruption on-site, the financial professional shall ensure that the third party in charge of this intervention is accompanied during the whole mission by an IT-staff member of the financial professional.

(g) Any financial professional shall designate one staff member who will be in charge of managing the access to confidential data.

(h) Whatever intervention is required on the programmes (advice, management, maintenance or modification), the third parties concerned may only work in a test environment and need the explicit agreement of the financial professional for each intervention, except if realised by a support PFS in the context of its mandate.

(i) For remote IT managed services, the financial professional shall ensure that sufficient protection measures are taken in order to avoid that unauthorised persons access its system. The financial professional shall ensure that telecommunications are encrypted or protected through other technical means available to ensure the security of communications.

The financial professional shall moreover ensure that measures are taken to allow normal functioning when lines are interrupted or dysrupted during an extended period of time.

4.5.2.2. The requirements on the IT function organisation are also considered as fulfilled by a financial professional whose datacenter is managed by an IT processing centre not belonging to it or of which it is only a co-owner and to which it is linked through telecommunication whenever the precise and restrictive conditions hereafter defined are met.

When the processing centre is located abroad, the outsourcing shall contractually be entrusted to the parent undertaking (or, in the case of branches, to the head office) or to a subsidiary of the parent undertaking or to a company specialised in IT processing controlled by the group to which the financial professional belongs. The entity responsible for the service provision must fall under the scope of the prudential supervision performed by a foreign supervisory authority. It is not mandatory for the

processing centre to be physically located on the premises of the responsible entity. Where the processing centre is physically located on the premises of or operated by a legal entity other than the one to which the processing has been entrusted with contractually, the financial professional shall ensure that the supervised entity, contractually responsible, complies with the principles indicated under point 4.5.2.1 The financial professional shall ensure to provide the CSSF with any elements allowing to prove that the sub-outsourcing process is under control. To this end, it shall present a document indicating the awareness of the other relevant supervisory authorities of this outsourcing, specifying whenever possible, the extent of their supervision in this context.

No confidential data allowing to identify a client of the financial professional must be stored within a processing centre other than a support PFS, unless it is encrypted and provided the decryption process can only be executed at the premises of the financial professional or of the support PFS in the context of its service provision.

When a datacentre is based in Luxembourg, it may be located within a company of the group which handles exclusively the group's operations, in accordance with article 13(2) of the Law, but in this case, it shall not contain any readable data that might allow the identification of the client. The datacentre may as well be located in a company that is jointly held and controlled by several Luxembourg financial professionals (banks or PFS) that cooperate in IT matters. In this case, the common centre exclusively processes operations on behalf of the financial professionals and must be licensed as a support PFS.

The financial professionals that consider having their data processed by an IT datacentre located abroad within a company subject to prudential supervision remain nevertheless responsible to maintain secrecy on the information entrusted to them in the context of their professional activity. Financial professionals are, in this context, subject to a greater disclosure risk than if using solutions specified under point 4.5.2.1 or appointing a support PFS.

A financial professional considering to rely on one of these organisations, other than a support PFS, shall seek the prior consent of the CSSF by proving that the conditions set out in this circular are satisfied.

Financial professionals intending to set up this type of structure, whether the service provider is a support PFS or not, shall comply with at least the following conditions in addition to those indicated under point 4.5.2.1:

(a) The IT link shall allow the Luxembourg financial professional to have a quick and unlimited access to information stored in the processing unit. Data input will be made entirely in the premises in Luxembourg through terminals. Data printing will be executed exclusively at the premises of the financial professional in Luxembourg or at a support PFS.

Nevertheless, data may be inputed or printed outside the premises of the financial professional by a client or a proxy initiating transactions through a telematic link.

The financial professional is required to have at the closing of each day the balance of all accounts and of all accounting movements of the day.

(b) The system shall allow to hold a regular accounting pursuant to the rules applicable in Luxembourg and thus respect the form and content ruled by the Luxembourg accounting principles.

(c) Communication between the financial professional and the datacentre shall be encrypted or protected by other technical means available to ensure the security of communication. No client name shall be inputed or registered in the system to which third parties, other than support PFS, have access.

(d) The external auditor and the internal audit department of the financial professional shall be in a position to assess the necessary controls in the datacentre in order to issue a well-founded opinion on the adequacy of the IT link.

(e) The IT link shall be set out in a service level agreement with requirement specifications which take into account the above conditions.

The financial professionals which currently have their data processed by means of such a link and which do not satisfy the above conditions are requested to contact the CSSF to present the measures it contemplates to take for the IT function to comply with the conditions set out in this circular.

4.5.2.3. Where the financial professional operates abroad relying on the services of professional intermediaries (even though they are part of the group to which the financial professional belongs) or where its representative

offices are located abroad, the intermediaries or representatives of these offices cannot, in any case, have access to its IT system in Luxembourg.

4.5.2.3. The requirements of control, quality and strict guarantee of confidential data protection imposed on financial professionals are fulfilled when the financial professional relies on a support PFS. In this case, the organisation shall be adapted in order to integrate the outsourced activities to the proper functioning of the financial professional and the procedures manual shall be adapted accordingly. The business continuity plan of the financial professional shall be established in accordance with the contingency plan of the support PFS.

The IT infrastructure may be owned by the financial professional or be provided by the support PFS. The staff of the support PFS may either work at its premises or at the premises of the financial professional.

The following specifications should be considered:

(a) The obligation to secrecy does not exist towards professionals referred to in Article 29-3 of the Law insofar as the information communicated to those professionals is provided in pursuance of a service level agreement falling within one of the activities regulated by the above-mentioned legal provisions, and provided that the information concerned is essential to the execution of the services provision in question. (Article 41(5))(b).

(b) The external auditor and the internal audit department of the financial professional shall be in a position to carry out the necessary controls on the premises of the support PFS to issue a well-founded opinion on the adequacy of the IT link. They may refer to the report of the external auditor of the support PFS, where applicable.

(c) A financial professional relying on a support PFS shall notify the CSSF by proving that the conditions laid down in this circular are satisfied.

5. <u>Assessment of the administrative and accounting organisation by the statutory auditor</u>

5.1. As regards banks, the long form report is to be established by the statutory auditor pursuant to Circular IML 89/60* shall include a description and a

* repealed by Circular CSSF 01/27 relating to practical rules concerning the role of statutory auditors.

point-to-point assessment of the rules relating to the administrative and accounting organisation as laid down in this Circular.

5.2. Branches of banks originating from the EC shall get item 4.5.2. of this Circular which concern them audited by their auditors on an annual basis. A report shall be addressed to the IML.

Yours faithfully,

INSTITUT MONETAIRE LUXEMBOURGEOIS

Jean GUILL
Director

JeanNicolas SCHAUS
Director