



Circular CSSF 04/155

as amended by Circular
CSSF 22/806

The compliance function

Circular CSSF 04/155 as amended by Circular CSSF 22/806

Re: The compliance function

Luxembourg, 27 September 2004

**To all electronic money
institutions and payments
institutions, to all specialised
PFS as well as POST
Luxembourg**

Dear Sir or Madam,

The purpose of this Circular is to clarify the way in which article 17(2) of the law of 5 April 1993 on the financial sector as amended (hereafter “**LFS**”), for specialised PFS¹ and POST Luxembourg and articles 11 (2) et 24-7 (2) of the law of 10 November 2009 on payment services (hereafter “**LPS**”) for payment institutions and electronic money institutions (hereafter collectively referred to “institutions”), by providing for the setting up of a “Compliance function” and by defining the way in which it shall work.

Chapter I. Introduction

1. In accordance with articles 17(2) of the LFS and articles 11(2) et 24-7(2) of the LPS, every institution shall prove that it has a sound administrative and accounting organisation, as well as adequate internal control procedures. These requirements include the setting up of a Compliance function in accordance with the principles set forth in this circular.

2. The Compliance function, as defined in Chapter III., contributes to the good functioning of the third level of control provided for by circular IML 98/143 on internal control as amended, i.e. of the controls performed by persons responsible for the daily management and authorised in accordance to articles 19(2) of the LFS and articles 13(2) and 24-9(2) of the LPS (hereinafter collectively referred to “senior management”) on the activities and/or functions under their direct responsibility. Thereby, compliance is a regular control associated with an on-going and close monitoring of the institution’s operations and related risks. The purpose of setting up a Compliance function is to organise, coordinate and structure compliance-related controls already carried out under the terms of other regulations, but which are currently often spread over several different organisational levels.

3. The Compliance function aims at protecting the institution from any prejudice that might result from the failure to comply with the rules in force, (as defined in Chapter III.), and at contributing to the efficient management of ensuing risks.

- ¹ By « specialised professional of the financial sector », reference is made to specialized professional of the financial sector which have decided to implement a compliance function within their institution.

4. Compliance is not of the sole remit of the Compliance function. Indeed, compliance with the rules applicable to the institutions is also a matter for the board of directors/board of managers, senior management, as well as staff members, and is thereby to be considered as a key element of the compliance culture of an institution. It follows that such a compliance- based culture shall be promoted within the institution.

Chapter II. Scope of the circular

5. Every institution under Luxembourg law shall set up a Compliance function which meets the principles laid down below. According to the arrangements set forth in Chapter XI., the circular also applies to branches of institutions under Luxembourg law and companies in which the institution holds a significant participating interest, which fall under the scope and limitations of supervision on a consolidated basis.

6. The circular also applies to Luxembourg branches of institutions whose head office is located outside the European Economic Area.

7. In order to ensure compliance with the rules applicable in the interest of the general good, including in particular those relating to the fight against money laundering and the financing of terrorism, the rules of conduct of the financial sector and the rules of protection of investor and client interests, as well as the regulations relating to the areas for which the Commission de Surveillance du Secteur Financier (CSSF) retains a responsibility as host country supervisor, Luxembourg branches of institutions of EU origin shall set up a compliance structure which aims at ensuring that the business activities are performed in accordance with the rules pertaining to the areas concerned.

Chapter III. Nature and purpose of the Compliance function

8. In order to promote a compliance-based culture, an institution shall draw up compliance principles. Compliance principles take the form of guiding rules based on judgement and experience and constitute a model of conduct for the institution. The compliance policy lays down the way these principles are implemented. The compliance charter lays down the way the Compliance function shall be organised in order for it to achieve its objectives.

9. The Compliance function is defined as an independent function whose objective is to identify and assess the compliance risk of an institution, as well as to assist senior management in managing and monitoring this risk. It reports to senior management and, where applicable, to the board of directors/board of managers and can act as advisor to senior management.

10. The expression “compliance risk” is defined as the risk of losses that an institution may suffer as a result of the failure to conduct its business in accordance with the rules in force. It can include a variety of risks such as reputation risk, legal risk, litigation risk, risk of sanctions, as well as certain aspects of operational risk, in relation with all the institution’s business activities.

11. The expression “*rules in force*” is defined in this context as the rules the institution shall comply with in the conduct of its business in the different markets, notably:

- the laws, regulations and circulars governing the access to the financial sector and the conduct of the regulated activities performed by the institution;
- the laws and circulars dealing with professional obligations, i.e. the rules concerning the fight against money laundering and the financing of terrorism, as well as the rules of conduct of the financial sector (in order to avoid, for instance, insider dealing and market price manipulation) and investor protection rules.

For the purpose of assessing the compliance risk and defining the scope of the Compliance function, internal codes of conduct or ethics, as well as codes of professional bodies and financial markets (stock markets or other regulated markets) shall also be taken into account.

12. It is a matter for the institution to decide whether, given the specificities of the activities performed, its Compliance function monitors compliance with rules not directly linked to the conduct of the regulated activities performed by the institution in the strict sense, such as rules pertaining to labour law, social legislation, company law or environmental law.

Chapter IV. Responsibilities of the board of directors/board of managers

13. The board of directors/board of managers is responsible for defining the compliance principles by which the institution shall abide in carrying out its activities. The board of directors shall promote a positive attitude with regard to compliance, promote the development of structures allowing to achieve this objective and ensure, at regular intervals, that the institution has an adequate Compliance function.

14. The compliance policy and charter drawn up by senior management shall be submitted for approval to the board of directors.

15. Within the scope of its supervisory responsibilities, the board of directors/board of managers shall assess, on a yearly basis, the way in which

the institution manages its compliance risk. To this end, it shall regularly, and at least once a year, obtain a report from senior management on compliance. The board of directors/board of managers may delegate its mission of regular assessment to the audit committee or to a Compliance committee specifically created for this purpose. As regards its composition, functioning and powers, such a compliance committee is subject to the same principles as the audit committee (referred to under point 6.c) of circular IML 98/143, as amended on internal control).

16. The board of directors/board of managers shall ensure that the Compliance function has, if needed, the right to directly contact the Chairman of the board of directors or, where applicable, the members of an audit committee or of a Compliance committee. It shall also ensure that the Compliance function has the right to have recourse on an ad-hoc basis to the services of external experts.

Chapter V. Responsibilities of senior management

17. Senior management is responsible for the drawing up and the implementation of the Compliance policy, as well as for the setting up of a Compliance function in accordance with the principles laid down in this circular.

18. It shall also ensure, on a regular basis, that the Compliance policy is appropriate and verify its implementation and respect thereof, which also implies that senior management decides, in the event of failure to comply with the policy or in case of serious deficiencies observed by the Compliance function, on the corrective measures, and where applicable, on the sanctions to be imposed.

19. Senior management informs, in such manner as it sees fit, and at least once a year, the board of directors/board of managers (where applicable, the audit committee or the Compliance committee) on the status of compliance.

20. In its report, senior management shall notably cover the achievement of the Compliance function's objectives, the human and technical means assigned to meet these objectives, the main observations resulting from the Compliance function's work, any deficiencies noted, the corrective measures taken and their follow-up, as well as any information allowing to determine if and how the Compliance function has carried out its responsibilities referred to under chapter IX.

21. Without prejudice to paragraph 17., senior management of the institution appoints one person among its members who shall be directly in charge of the Compliance function. The name of this person, as well as any related change shall be communicated by senior management to the CSSF.

Chapter VI. The Compliance policy

22. Every institution shall have a Compliance policy, established and regularly updated by senior management and approved by the board of directors/board of managers.

23. This Compliance policy is laid down in writing. It shall contain the main aspects of the compliance risk, explain the principles laid down by the board of directors/board of managers, establish the Compliance function and define its goals and independence, require the drawing up of a charter, and institute the implementation of a continuous training programme.

24. The policy need not detail all the laws, regulations, circulars and other applicable codes, but it shall lay down the main principles to follow. The policy serves as framework for the implementation of the Compliance function and of the detailed and specific procedures or instructions.

Chapter VII. Compliance Charter

25. The way in which the Compliance function operates shall be laid down by a compliance charter approved by senior management and the board of directors/board of managers.

26. The charter shall at least:

- set forth the objectives of the Compliance function;
- define its responsibilities and role;
- establish its independence and permanence;
- describe the relationship with other departments and functions as well as any need of outsourcing², delegation and/or coordination;
- grant the Compliance function the access right to any information necessary to carry out its responsibilities;
- acknowledge its right to conduct investigations;
- define the reporting lines;
- establish the right to contact senior management, and, where applicable, the Chairman of the board or the members of an audit committee or a Compliance committee;
- define the conditions in which the function can have recourse on an ad-hoc basis to external experts.

² Please refer to the Circular CSSF 22/806 related to outsourcing concerning the outsourcing arrangements of the internal control functions as well as any other related topics.

27. The compliance charter shall evolve and be updated promptly to take account of the changes to the rules applicable to the institution. All the changes shall be approved by the board of directors. Furthermore, the compliance charter, as well as any subsequent changes thereto shall be brought to the knowledge of all staff.

Chapter VIII. Organisation of the Compliance function

28. In accordance with the requirements set forth in chapter VII., every institution shall organise its Compliance function so as to meet the following requirements:

a) Independence

The Compliance function shall not be accountable to a division or department of the institution but shall have a direct reporting line to the institution's senior management.

It shall be able to carry out its role and responsibilities on its own initiative.

b) Resources

The institution shall organise its Compliance function in such a way as to enable it to carry out its responsibilities in an adequate and permanent manner.

It shall also have the necessary human resources to perform its duties. The size of the function shall be commensurate with the size of the institution, as well as with the nature and complexity of its activities.

The institution appoints one employee responsible for managing the Compliance function generally known as "Compliance Officer".

The name of this employee, as well as any subsequent change relating to this appointment, shall be notified to the CSSF.

Notwithstanding the abovementioned requirements, the institution has a certain flexibility as regards the organisation of its Compliance function:

ba) Some of the duties related to the responsibilities referred to under chapter IX. may be delegated to departments, units or divisions. In this case, the Compliance function takes on a coordinating role between the units performing the duties ensuing from the responsibilities described under chapter IX.

The Compliance charter shall clearly state the relationships between the different intervening units. It shall notably state that the Compliance function remains responsible for the duties delegated. The institution ensures that the delegated duties remain compatible with the other duties that the persons of the other units carry out.

bb) Where neither the size of the institution, nor the nature of its activities, nor the risks incurred require the creation of a full-time position of Compliance Officer, a person can be assigned on a part-time basis.

Care must be taken to ensure that the other responsibilities performed by this employee remain compatible with the responsibilities performed under the terms of this circular.

An institution wishing to dispense with the creation of a full-time Compliance Officer position shall obtain explicit authorisation from the CSSF. To this end, it shall submit a written request, providing a justification and the necessary information allowing to ensure that the provisions of this circular are adequately complied with, and that the Compliance function is performed appropriately.

bc) It is acceptable, subject to specific authorisation of the CSSF, that the member of senior management in charge of the Compliance function (according to paragraph 21. of Chapter V.) takes up the position of the Compliance Officer.

bd) The Compliance function shall not be outsourced. This principle shall not preclude the possibility to outsource operational tasks of the compliance function or to use on ad-hoc basis the expertise or technical means of third parties as provided for under point c) hereunder.

This circular, and this paragraph in particular have to be read in conjunction with the circular CSSF 22/806 related to outsourcing concerning the outsourcing arrangements of the internal control functions as well as any related topics. Please refer notably to paragraph 21 and 24 of circular CSSF 22/806.

c) Competence

In order to guarantee the efficiency of the Compliance function, its members shall have a high degree of professional qualification in the area the regulated activities performed by the institution and the rules in force.

The competence of the members of the Compliance function shall be appraised by taking account not only of the nature of their duties but also of the complexity and diversity of the institution's business activities.

These provisions do not preclude the Compliance function from having recourse on ad-hoc basis to the expertise or technical means of third parties for certain specific aspects. Every institution takes the appropriate measures to ensure that the Compliance function staff carries out its duties with integrity and discretion.

d) Delegation and coordination

A formalisation of the delegation, as laid down in the compliance charter, is necessary namely for institutions where the Compliance function takes on a role of coordination as referred to under the aforementioned

point ba) and where the performance of the tasks themselves is carried out by other organisational units.

The Compliance Officer consults, on a regular basis, with the representatives of departments contributing to the Compliance function's operations, but also with any department that is particularly exposed to a compliance risk. The purpose of this consultation is notably to ensure proper implementation of the compliance policy.

Chapter IX. Responsibilities of the Compliance function

29. In order to achieve its objectives, the responsibilities of the Compliance function shall at least cover the following aspects:

a) Identification and assessment of the compliance risk

The Compliance function identifies the compliance risks to which the institution is exposed within the course of its business and assesses their significance, as well as their potential consequences.

The Compliance function sees to the identification and assessment of the compliance risk before the institution starts a new type of activity, product or business relationship, as well as in the event of the development of group business and network at international level.

b) Identification of the rules in force

The Compliance function identifies the rules referred to under paragraph 11. of this circular and keep a list of the main rules governing the performance of the institution's activities. This list shall be available to the staff concerned.

c) Procedures and instructions for the implementation of the compliance policy

As far as the implementation of the Compliance policy is concerned, the Compliance function ensures that the institution has rules that may be used as guidelines for staff of the different business lines for the performance of their day-to-day duties.

These rules shall be appropriately reflected in the instructions, procedures and internal controls for those areas pertaining directly to Compliance (such as for instance the fight against money laundering and the protection of client and investor interests). In drawing up these rules, the Compliance function takes account, as far as appropriate for the institution concerned, of the codes of ethics described under the last indent of paragraph 11.

As far as the areas that do not directly pertain to Compliance are concerned, the Compliance function is involved and consulted at the time of drawing up and the implementation of the internal control procedures.

d) Monitoring of the respect of the Compliance policy

The Compliance function regularly monitors compliance with the compliance policy, procedures and instructions, and proposes corrective measures where appropriate. To this end, the Compliance function assesses and controls the Compliance risk on a regular basis. As regards the controls concerning compliance risk and the monitoring of the procedures and instructions, the provisions of this circular do not prevent the Compliance function from relying on the works of internal audit.

e) Centralisation of information on compliance issues

The Compliance function centralises all the information on Compliance issues (i.e. breaches of rules, non-compliance with procedures, conflicts of interests, etc.) observed within the institution.

As far as this information is not the product of its own involvement, the Compliance function shall conduct an examination of relevant documents, be they internal documents (i.e. internal control or internal audit reports, reports or minutes of senior management or, where applicable, of the board of directors) or external documents (i.e. reports of the external auditor, correspondence from the supervisory authority).

f) Analysis of Compliance issues, interventions and follow-up

The Compliance functions analyses the issues observed and recommend, where applicable, corrective measures to address these deficiencies.

It follows up on the issues previously observed and ensure that the corrective measures haven been implemented appropriately and have proven to be efficient.

g) Assistance and advice to senior management in Compliance matters

The Compliance function assists and advises senior management on issues concerning compliance and rules, notably by informing the latter about developments regarding regulations which might subsequently have an impact on the area of compliance.

h) Awareness and training of staff

The Compliance function raises the awareness of staff as to the importance of Compliance and related aspects. To this end, it develops a training programme and sees to its implementation.

i) Communication with authorities

The Compliance Officer is responsible for fulfilling the notification requirements to the authorities as laid down in the laws, regulations and circulars relating to the fight against money laundering and the prevention of the use of the financial sector for money-laundering purposes.

j) Documentation of the work and internal reporting

The Compliance function documents the work carried out in accordance with the responsibilities assigned, notably in order to allow to track the interventions as well as the conclusions drawn.

It reports, in a form it sees fit, to senior management and, where applicable, to the board of directors/board of managers (or to an audit or Compliance committee) significant issues and deficiencies observed as regards procedures or even the compliance policy, as well as any measures taken.

Besides ad hoc reports, the Compliance function regularly draws up a report for senior management on its activities and its functioning. This report lists significant issues that have occurred since the last report, as well as corrective measures taken and shall inform senior management on the investigations carried out, as well as on the activities with regard to the other responsibilities described in this chapter.

Chapter X. Control of the Compliance function by internal audit

30. The activities of the Compliance function shall be part of the scope of intervention of internal audit. Internal audit shall assess the functioning and efficiency of the Compliance function.

31. In the light of the above, the Compliance function cannot be part of the internal audit function of an institution. However, this does not prevent internal audit from taking on an executive role in the verification of the proper application of the rules in force to the activities carried out by an institution.

Chapter XI. Application of this circular to institutions with branches and to groups of institutions

32. The Compliance function of an institution under the terms of and according to the provisions of this circular shall also be set up at a consolidated level

encompassing notably the branches, that this institution holds in the Grand Duchy of Luxembourg or abroad.

33. For institutions with branches or subsidiaries abroad, the implementation of the Compliance policy in these establishments shall take account of the rules in force at local level.

34. The subsidiaries and branches of a certain size shall have their own Compliance function. The Compliance function of the branch is accountable, from a hierarchical and functional point of view, to the Compliance function of the head office to which it belongs and reports. For subsidiaries, the reports established in accordance with the provisions of this circular shall not only be submitted to the local governing bodies, but also, in summary form, to the Compliance function of the Luxembourg parent company which analyses and reports on the issues to be addressed. Senior management of the Luxembourg parent company establishes general rules as regards compliance for its subsidiaries as well as for its branches.

35. In the case of companies of a certain size in which an institution holds a participating interest between 20% and 50%, the Luxembourg institution, which is not parent company, shall do its utmost, in conjunction with the other shareholders and partners concerned, that a Compliance function which shall meet standards comparable to those prescribed by this circular be set up in these institutions, notwithstanding the local rules in this field. The Luxembourg institution endeavours to obtain a summary Compliance report of the companies concerned and have them analysed by its own Compliance function. The latter reports on the main deficiencies observed, the corrective measures taken and the follow-up of these measures.

36. The principles of this circular do not preclude, for Luxembourg institutions that are branches or subsidiaries of professionals of the financial sector located in Luxembourg or abroad, having a Compliance function at group level, from linking their local Compliance function to that of the group. Such a functional link may notably be used to share expertise and technical means among the different entities of the group; it is also the basis for a co-operation and coordination in a consolidated Compliance approach.

Chapter XII. Reporting to the Commission de Surveillance du Secteur Financier

37. On a yearly basis, the institutions include in the reports submitted to the CSSF in accordance with circular IML 98/143, as amended on internal control, information on the status of the Compliance function, as well as on the main observations made in this context (notably covering the deficiencies observed, the corrective measures taken, as well as their follow-up).

Chapter XIII. Assessment of the Compliance function

38. In accordance with circulars CSSF 12/550 and 13/569 on external audit guidelines in practice, the long form report of the institutions falling within the scope of this circular, shall include a description and assessment of the Compliance function.

39. Where an institution is exempt from drawing up a long form report, the management letter of the external auditor shall mention, where applicable, any failure to comply with the provisions relating to the Compliance function as laid down by this circular.

Chapter XIV. Coming into force

40. This circular shall come into force with immediate effect.



Commission de Surveillance du Secteur Financier
283, route d'Arlon
L-2991 Luxembourg (+352) 26 25 1-1
direction@cssf.lu
www.cssf.lu