cssf

Commission de Surveillance
du Secteur Financier

Circular CSSF 20/758

as amended by Circulars CSSF 21/785 and CSSF 22/806

Central administration, internal governance and risk management

Commission de Surveillance du Secteur Financier

Circular CSSF 20/758 as amended by Circulars CSSF 21/785 and CSSF 22/806

Re: Central administration, internal governance and risk management

Luxembourg, 7 December 2020

To all investment firms

Ladies and Gentlemen,

Articles 17(1a) and 38-1 of the Law of 5 April 1993 on the financial sector ("LFS"), supplemented by Regulation CSSF No 15-02 relating to the supervisory review and evaluation ("RCSSF 15-02")[1] require investment firms to have robust internal governance arrangements, which shall include a clear organisational structure with well-defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks to which they are or might be exposed, adequate internal control mechanisms, including sound administrative and accounting procedures and remuneration policies and practices allowing and promoting sound and effective risk management, as well as control and security mechanisms for their IT systems.

This Circular specifies the measures investment firms must take pursuant to the provisions of the LFS and RCSSF 15-02[2] as regards central administration, internal governance and risk management. It reflects the European and international principles, guidelines and recommendations which apply in this respect, translating them, in a proportionate way, in the context of the Luxembourg financial sector. Where, due to the size, the nature and the complexity of the activities and the organisation, the application of the principle of proportionality requires enhanced central administration, internal governance or risk management, the institutions shall refer to the principles set out in Chapter 2 of Part I and to the above-mentioned guidelines and recommendations for guidance on this implementation. This concerns especially the European Banking Authority ("EBA") Guidelines on internal governance (EBA/GL/2017/11) and the joint EBA and the European Securities and Markets Authority ("ESMA") Guidelines on the assessment of the suitability of members of the management body and key function holders (EBA/GL/2017/12).

This Circular repeals and replaces Circular CSSF 12/552 on central administration, internal governance and risk management (as amended by Circulars CSSF 13/563, CSSF 14/597, CSSF 16/642, CSSF 16/647, CSSF 17/655 and CSSF 20/750) with regard to investment firms.

[1] *RCSSF 15-02 only applies to CRR institutions, i.e. to credit institutions and CRR investment firms.*

[2] *Idem*

Commission de Surveillance du Secteur Financier

As regards the appointments of directors, authorised managers and key function holders, this Circular should be read in conjunction with the Prudential Procedure in this respect published on the CSSF website.

The Circular is divided into four parts: the first part contains definitions and establishes the scope, the second part is dedicated to central administration and internal governance requirements, the third part covers specific risk management requirements and the fourth part provides for the entry into force of this Circular.

Commission de Surveillance du Secteur Financier

TABLE OF CONTENTS

Commission de Surveillance du Secteur Financier

Part I - Definitions and Scope

Chapter 1. Definitions and abbreviations

1. For the purposes of this Circular:
   1) "Board of Directors" shall mean the body or, failing that, the persons who, under company law, monitor the management by the authorised management. According to the financial sector regulation, Boards of Directors of investment firms are assigned responsibilities as regards the supervision and control, as well as the determination and approval of strategies and key policies. The term "Board of Directors" shall not be understood in its legal sense as investment firms can also take a legal form which does not provide for a "Board of Directors" within the meaning of company law. For instance, in a two-tier structure, the Board of Supervisors shall assume the responsibilities that this Circular assigns to the "Board of Directors". The Board of Directors shall also correspond to the management body, in its supervisory function, according to EBA/GL/2017/11.
   2) "authorised management" or "authorised managers" shall mean the persons referred to in Article 19(2) of the LFS. From a prudential standpoint, the authorised management shall be in charge of the day-to-day management of an investment firm, in accordance with the strategic directions and the key policies approved by the Board of Directors. The authorised management shall also be considered as the management body, in its management function, according to EBA/GL/2017/11.

      In a one-tier system, the authorised managers may be members of the Board of Directors, while in a two-tier system, the authorised management corresponds to the Executive Board.

   3) "CRR investment firm" shall mean an investment firm within the meaning of point (2) of Article 4(1) of Regulation (EU) No 575/2013.
   4) "non-CRR investment firm" shall mean an investment firm other than a CRR investment firm.
   5) "institution(s)" or "investment firm(s)" shall mean CRR and non-CRR investment firms incorporated under Luxembourg law, including their branches and the Luxembourg branches of third-country investment firms, as well as Luxembourg branches of investment firms authorised in another Member State.

6) "significant institution" shall, for the purposes of this Circular, mean a systemically important investment firm in accordance with Article 59-3 of the LFS and, if applicable, other investment firms determined as such by the CSSF based on the assessment of the investment firms' size and internal organisation as well as the nature, the scale and the complexity of their activities.
7) "outsourcing" shall mean an arrangement of any form concluded between an institution and a service provider by which that service provider performs a process a service or an activity that would otherwise be undertaken by the institution itself.
8) "ICAAP" shall mean Internal Capital Adequacy Assessment Process.
9) "ILAAP" shall mean Internal Liquidity Adequacy Assessment Process.
10) "LFS" shall mean the Law of 5 April 1993 on the financial sector, as amended.
11) "MiFID" shall mean the Markets in Financial Instruments Directive.
12) "management body" shall mean the management body, in accordance with the definition of the LFS, and shall be the management body in its supervisory function and in its management function in accordance with EBA/GL/2017/11. It shall refer to the Board of Directors and the authorised management of an institution with a one-tier structure or the Supervisory Board and the Executive Board of an institution with a two-tier structure.
13) "related parties" shall mean the legal entities (structures) which are part of the group to which the institution belongs as well as the staff members, shareholders, managers and members of the Board of Directors of these entities.
14) "Prudential Procedure" shall mean the prudential procedure for the approval of directors, authorised managers and key function holders in investment firms.
15) "CRR" shall mean Regulation (EU) No 575/2013 of 26 June 2013 on prudential requirements for credit institutions and investment firms.
16) "key function holders" shall mean the heads of functions whose performance allows a significant influence over the conduct or monitoring of the activities of the institutions. They include, in particular, the heads of the three internal control functions in all institutions, i.e. the Chief Risk Officer ("CRO") for the risk control function, the Chief Compliance Officer ("CCO") for the compliance function and the Chief Internal Auditor ("CIA") for the internal audit function, as well as the head of the financial function (Chief Financial Officer, "CFO") in significant institutions.

Chapter 2. Scope and proportionality

2. This Circular shall apply to investment firms incorporated under Luxembourg law, including their branches, as well as the Luxembourg branches of third-country investment firms.

   In respect of the areas for which the CSSF retains an oversight responsibility as host authority – i.e. anti-money laundering and counter terrorist financing measures and rules applicable to the provision of investment services – Luxembourg branches of investment firms authorised in another Member State, in coordination with this authorised firm, shall establish central administration, internal governance and risk management arrangements which are comparable to those provided for in this Circular.

3. This Circular shall apply to institutions, on a stand-alone, sub-consolidated and consolidated basis, to financial holding companies or mixed financial holding companies referred to in points (a) to (c) of Article 49(2) of the LFS.

   If the institution is a parent undertaking (group head), the Circular shall then apply to "the group" as a whole: to the parent undertaking and the various legal entities that are part of this group - whether or not they are included in the scope of prudential consolidation according to the CRR - including the branches, in compliance with the national laws and regulatory provisions which apply to the entities in question.

   Thus, whatever the organisational and operational structure of the institution or a group, the implementation of this Circular shall enable the institution to have complete control over its activities and the risks to which it is or may be exposed, including the intra-group activities and risks and regardless of the location of the risks.

   Proportionality shall apply to the implementing measures, which the institutions take pursuant to this Circular, having regard to the nature, scale and complexity of their activities, including the risks. In practice, the application of the principle of proportionality implies that the institutions which are more significant, complex or riskier have in place enhanced central administration, internal governance and risk management arrangements. These enhanced arrangements shall include, for example, the establishment of specialised committees, the appointment of independent members additional to the Board of Directors or additional authorised managers to facilitate the day-to-day management.

Conversely, for institutions which are smaller in size and internal organisation, whose activities are minor in terms of nature, scale and complexity, the principle of proportionality could be applied downward. Thus, an institution with limited activities of low complexity may operate properly within the meaning of this Circular by designating heads of compliance and risk control functions on a part-time basis (without questioning the principle of permanence of the function) or by fully or partially outsourcing the performance of the operational tasks of the internal control functions, including the internal audit function. The downward application of the principle of proportionality is limited, in particular, by the principle of segregation of duties under which the duties and responsibilities must be assigned so as to avoid conflicts of interest involving the same person.

While the allocation of tasks within the authorised management is done in compliance with the principle of segregation of duties, joint responsibility shall be maintained.

The implementation of the principle of proportionality shall take account of the following:

a. the legal form and the ownership and funding structure of the institution;
b. the business model and risk strategy;
c. the size of the institution and its subsidiaries as well as the nature and complexity of the activities (including the type of customers and the complexity of the products and contracts);
d. the nature and complexity of the organisational and operational structure, including the geographic footprint, the distribution channels and the outsourced functions;
e. the nature and state of the IT systems and continuity systems.

Regardless of the adopted organisation, the arrangements in this respect shall enable the institution to operate in full compliance with the provisions of Part II of this Circular. The institutions shall document their proportionality analysis in writing and have their conclusions approved by the Board of Directors.

Commission de Surveillance du Secteur Financier

Part II. Central administration and internal governance arrangements

Chapter 1. Central administration

1. The institutions shall have a robust central administration in Luxembourg, consisting of their "decision-making centre" and their "administrative centre". The central administration, which shall comprise, in a broad sense, the executive, management, execution and control functions, shall enable the institution to retain control over all of its activities.

2. The decision-making centre shall include the authorised management and the heads of the business functions, the support and control functions and the various business units existing within the institution.

3. The administrative centre shall include the administrative, accounting and IT organisation which shall ensure, at all times, proper administration of securities and assets, adequate execution of operations, accurate and complete recording of operations and production of accurate, complete, relevant and understandable management information available without delay.

4. Where the institution is the group head, the central administration shall enable the institution to concentrate any management information necessary to manage, monitor and control the activities of the group, on an ongoing basis, within its head office in Luxembourg. Similarly, the central administration shall enable the institution to reach all legal entities and branches which are part of the group in order to provide them with any necessary management information. The concept of management information shall be understood in the broadest possible sense, including financial information and legal reporting.

Chapter 2. Internal governance arrangements

5. Internal governance is a crucial component of the corporate governance framework, focussing on the internal structure and organisation of an institution. Corporate governance is a broader concept which may be described as the set of relationships between an institution, its Board of Directors, its authorised management, its shareholders and the other stakeholders.

6. Internal governance must ensure a sound and prudent management of the activities, including of inherent risks. The internal governance arrangements shall include:

- a clear and consistent organisational and operational structure with decision-making powers, reporting and functional lines and share of responsibility which are well-defined, transparent, consistent, complete and free from conflicts of interest;
- adequate internal control mechanisms which comply with the provisions of Chapter 6 of this part. These mechanisms shall include sound administrative, accounting and IT procedures and remuneration policies and practices allowing and promoting sound and effective risk management, in line with the institution's risk strategy, as well as control and security mechanisms for management information systems. The concept of management information system shall include IT systems;
- a clear risk-taking process including a risk appetite that is formally and precisely defined in all the business areas, a rigorous decision-making process and quality and limit analyses;
- processes to identify, measure, report, manage, mitigate and control the risks to which the institutions are or may be exposed;
- a management information system, including as regards risks, as well as internal communication arrangements comprising an internal alert procedure (whistleblowing) which enables the institution's staff to draw the heads' attention to all their significant and legitimate concerns about the internal governance of the institution;
- a formal escalation, settlement and sanction procedure for the problems, shortcomings and irregularities identified through the internal control and alert mechanisms;
- business continuity management arrangements aimed to limit the risks of severe business disruption and to maintain the key operations as defined by the Board of Directors upon proposal of the authorised management. These arrangements shall include a business continuity plan which describes the actions to be taken in order to continue to operate in case of an incident or disaster;
- crisis management arrangements which ensure appropriate responsiveness in the event of a crisis, including a recovery plan in accordance with the requirements of Chapter 2 of Part IV of the LFS.

7. Any institution shall promote an internal risk and compliance culture in order to ensure that all the institution's staff take an active part in the internal control as well as in the identification, reporting and monitoring of the risks incurred by the institution and develop a positive approach to the internal control.

This strong and ubiquitous overall risk and compliance culture must also be reflected in the strategies, policies and procedures of the institution, the training offered and the messages brought to staff members as regards the risk-taking and the risk management within the institution. Such culture shall be characterised by the example the Board of Directors and the authorised management set ("tone from the top") and requires all staff members to be accountable for their acts and behaviour, an open and critical dialogue and the absence of an incentive for inappropriate risk-taking.

Chapter 3. General characteristics of "robust" central administration and internal governance arrangements

8. Central administration and internal governance arrangements shall be developed and implemented so that they:
   - operate with "integrity". This part includes both the management of conflicts of interest and the security, in particular, as regards information systems;
   - are reliable and operate on an ongoing basis ("robustness"). Pursuant to the principle of continuity, any institution shall also establish arrangements aimed to restore the operation of the internal governance arrangements in case of discontinuity;
   - are effective ("effectiveness"). Effectiveness is given, in particular, when risks are effectively managed and monitored;
   - meet the needs of the institution as a whole and of all its organisational and business units ("adequacy");
   - are consistent as a whole and in their parts ("consistency");
   - are comprehensive ("comprehensiveness"). In respect of risks, comprehensiveness shall mean that all risks must be included within the scope of the internal governance arrangements. This scope shall not be limited to the sole (consolidated) prudential or accounting scope. This scope shall enable the institution to have a thorough overview of all its risks, in terms of economic substance, considering all the interactions existing throughout the institution. In respect of the internal control, the principle of comprehensiveness implies that the internal control shall apply to all areas of operation of the institution;
   - are transparent ("transparency"). Transparency shall include a clear and visible assignment and communication of the roles and responsibilities to the different staff members, the authorised management and the business and organisational units of the institution;
   - comply with the legal and regulatory requirements, including with the requirements of this Circular ("compliance").

9. In order to ensure and maintain the robustness of the central administration and internal governance arrangements, these shall be subject to objective, critical and regular review at least once a year. This review shall consider all internal and external changes which may have a significant adverse effect on the robustness of these arrangements as a whole and on the risk profile, and in particular on the institution's ability to manage and bear its risks.

10. The CRR investment firms shall disclose the key elements on internal governance and risk management in accordance with the provisions of the CRR (Article 435 and Title I of Part Eight) and the EBA Guidelines on disclosure requirements under Part Eight of Regulation (EU) No 575/2013 ("EBA/GL/2016/11").

Chapter 4. Board of Directors and authorised management

Sub-chapter 4.1. Board of Directors

Section 4.1.1. Responsibilities of the Board of Directors

11. The Board of Directors shall have the overall responsibility for the institution. It shall define, monitor and bear responsibility for the implementation of robust central administration, governance and internal control arrangements, which shall include a clearly structured internal organisation and independent internal control functions with appropriate authority, stature and resources with respect to their responsibilities. The implemented framework must ensure the sound and prudent management of the institution, preserve its continuity and protect its reputation. To this end, after having heard the authorised management and the heads of the internal control functions, the Board of Directors shall approve and lay down, in writing, the following key elements of the central administration, internal governance and risk management arrangements:
    - the business strategy (business model) of the institution, considering the institution's long-term financial interests, solvency, liquidity situation and risk appetite. The development and maintenance of a sustainable business model requires that account be taken of all material risks, including environmental, social and governance risks;
    - the risk strategy of the institution, including the risk appetite and the overall framework for risk-taking and risk management of the institution;
    - the strategy of the institution with respect to regulatory and internal capital and liquidity reserves;
    - a clear and consistent organisational and operational structure which shall govern, in particular, the creation and maintenance of legal entities (structures) by the institution;

- the guiding principles as regards information systems, technology and security in accordance with Circular CSSF 20/750, including the internal communication and alert arrangements;
- the guiding principles relating to the internal control mechanisms, including the internal control functions;
- the guiding principles relating to the remuneration policy;
- the guiding principles relating to professional conduct, corporate values and the management of conflicts of interest;
- the guiding principles relating to escalation and sanctions the purpose of which is to ensure that any behaviour which does not comply with the applicable rules is properly investigated and sanctioned;
- the guiding principles relating to the central administration in Luxembourg, including:
  - the human and material resources which are required for the implementation of the organisational and operational structure as well as the institution's strategies;
  - an administrative, accounting and IT organisation with integrity, and complying with the applicable laws and standards;
  - the guiding principles relating to outsourcing, including IT-related outsourcing, whether or not it is based on a cloud computing infrastructure, and
  - the guiding principles governing the change in activity (in terms of market coverage and customers, new products and services) and the approval and maintenance of non-standard or potentially non-transparent activities;
- the guiding principles relating to business continuity and crisis management, and
- the guiding principles governing the appointment and succession to the Board of Directors, the authorised management and key function holders in the institution, as well as the procedures governing the composition of the Board of Directors, including the aspects of diversity, responsibilities, organisation, operation, and individual and collective assessment of its members.[3] The aspects of diversity shall refer to the characteristics of the members of the management body, including their age, gender, geographical origin and educational and professional background. The promotion of diversity shall be based on the principle of non-discrimination and on measures ensuring equal opportunities.

[3] *In compliance with corporate governance, the guiding principles and procedures applicable to the members of the Board of Directors are, where appropriate, submitted to the shareholders for approval.*

12. The Board of Directors shall entrust the authorised management with the implementation of the strategies and guiding principles through internal written policies and procedures (except for the guiding principles governing the appointment and succession within the Board of Directors and the procedures determining its operation).

13. The Board of Directors shall monitor the implementation by the authorised management of the strategies and guiding principles and approve the policies established by the authorised management according to these strategies and principles.

14. The Board of Directors shall critically assess, adapt, where necessary, and re-approve, on a regular basis and at least once a year, the internal governance arrangements, including the key strategies and guiding principles and their implementation within the institution, the internal control mechanisms and the framework for risk-taking and risk management. These assessments and re-approvals aim to ensure that the internal governance arrangements continue to comply with the requirements of this Circular and the objectives of effective, sound and prudent business management.

    The assessment and re-approval by the Board of Directors shall relate, in particular, to the following:

    - the correlation between the incurred risks, the institution's ability to manage these risks and the internal and regulatory capital and liquidity reserves, in line with the strategies and guiding principles established by the Board of Directors and the applicable regulations, including Circular CSSF 11/506;
    - the strategies and guiding principles in order to improve them and to adapt them to internal and external, current and anticipated changes, as well as to the lessons learnt from the past;
    - the manner in which the authorised management meets its responsibilities and the performance of its members. In this context, the Board of Directors shall critically and constructively review and assess the actions, proposals, decisions and information provided by the authorised management and shall, in particular, ensure that the authorised management promptly and efficiently implements the corrective measures required to address the problems, shortcomings and irregularities identified by the internal control functions, the *réviseur d'entreprises agréé* (approved statutory auditor), the CSSF and, where applicable, another competent authority;

- the adequacy of the organisational and operational structure. The Board of Directors must fully know and understand the organisational structure of the institution, in particular of the underlying legal entities (structures), their raison d'être, the intra-group links and interactions as well as the risks related thereto. It shall verify that the organisational and operational structure complies with the strategies and guiding principles, that it enables a sound and prudent business management which is transparent and free from undue complexity, and that it remains justified in relation to the assigned objectives. This requirement shall apply, in particular, to non-standard or potentially non-transparent activities;
- the effectiveness and efficiency of the internal control mechanisms put in place by the authorised management.

The assessments in question may be prepared by specialised committees. These assessments shall, in particular, be based on the information received from the authorised management, the audit reports issued by the *réviseur d'entreprises agréé* (reports on annual accounts, long form reports and, where appropriate, management letters), the ICAAP/ILAAP reports and the reports of the internal control functions which the Board of Directors is called upon to approve on this occasion.

15. The Board of Directors shall be in charge of promoting an internal risk and compliance culture which raises the awareness of the institution's staff as regards the requirements of a sound and prudent risk management and which fosters a positive attitude towards internal control and compliance. It shall also be in charge of stimulating the development of internal governance arrangements which allow reaching these objectives.

    In respect of the internal control functions, the Board of Directors shall ensure that the work of these functions is performed in compliance with the recognised standards and under the approved policies.

16. The Board of Directors shall ensure that sufficient time is devoted to risk issues.

17. Where the Board of Directors becomes aware that the central administration or internal governance arrangements no longer ensure a sound and prudent business management or that the incurred risks are or will no longer be adequately borne by the institution's ability to manage these risks, by the internal or regulatory capital or liquidity reserves, it requires the authorised management to provide it with the corrective measures, without delay, and to inform the CSSF thereof forthwith. The obligation to notify the CSSF also concerns all information which casts doubt on the qualification or good repute of a member of the Board of Directors or the authorised management or a head of a key function.

Section 4.1.2. Composition and qualification of the Board of Directors

18. The members of the Board of Directors must be in sufficient number and, as a whole, must be composed adequately so that the Board of Directors can fully meet its responsibilities. The adequacy of the composition of the Board of Directors refers, in particular, to professional qualifications (adequate knowledge, skills and experience), as well as to the personal qualities of the members of the Board of Directors. The personal qualities shall be those which enable them to effectively perform their mandate with the required commitment, availability, objectivity, critical thinking and independence of mind. Moreover, each member shall demonstrate his/her professional repute. The guiding principles governing the appointment and succession of the members of the Board of Directors explain and provide for the abilities deemed necessary to ensure an appropriate composition and qualification of the Board of Directors.

19. The Board of Directors must collectively have appropriate knowledge, skills and experience with regard to the nature, scale and complexity of the activities and the organisation of the institution.

    Collectively, the Board of Directors must fully know and understand all the activities (and inherent risks) as well as the economic and regulatory environment in which the institution operates.

    Each member of the Board of Directors shall have a complete understanding of the internal governance arrangements and his/her responsibilities within the institution. The members shall control the activities which fall within their areas of expertise and shall have a good understanding of the other significant activities of the institution.

20. The members of the Board of Directors shall ensure that their personal qualities enable them to perform their mandate effectively, with the required commitment, availability, objectivity, critical thinking and independence of mind. In this respect, the Board of Directors cannot have among its members a majority of persons who take on an executive role within the institution (authorised managers or other staff members of the institution, with the exception of staff representatives elected in accordance with the applicable regulations).

    The members of the Board of Directors shall ensure that their mandate is and remains compatible with any other positions, mandates and interests they may have, in particular in terms of conflicts of interest and availability. They shall inform the Board of Directors of the mandates they have outside the institution.

21. The terms of reference of the directors' mandates must be laid down so that the Board of Directors may fulfil its responsibilities effectively and on an ongoing basis. The renewal of the existing members' mandates must, in particular, be based on their past performance. Continuity in the functioning of the Board of Directors must be ensured.

22. The guiding principles governing the appointment and succession of the members of the Board of Directors provide for the measures required in order for these members to be and remain qualified throughout their mandate. These measures include a specific initiation to understand the structure, the business model, the risk profile and the governance arrangements, and then vocational training programmes which enable members of the Board of Directors, on the one hand, to understand the operations of the institution, their role and, on the other hand, to update and develop their skills.

23. In principle, each CRR investment firm should appoint at least one member to its Board of Directors who may be considered as "independent member".

    An independent member of the Board of Directors shall not have any conflict of interest which might impair his/her judgement because s/he is or has been, in the recent past, bound by any professional, family or other relationship with the institution, its controlling shareholder or the management of either. As to the assessment of "being independent", the institutions shall apply the criteria of Section 9.3 of EBA/GL/2017/12 as provided for in Annex I.

    The significant institutions or the institutions whose shares are admitted to trading on a regulated market shall ensure that their Board of Directors has a sufficient number of independent members, considering their organisation and the nature, the scale and the complexity of their activities.

Section 4.1.3. Organisation and functioning of the Board of Directors

24. The Board of Directors shall regularly meet in order to effectively fulfil its responsibilities. The organisation and functioning of the Board of Directors shall be documented in writing. The objectives and responsibilities of its members shall also be documented by way of written mandates.

25. The work of the Board of Directors must be documented in writing. This documentation shall include the agenda and minutes of the meetings as well as the decisions and measures taken by the Board of Directors. The minutes are an important tool which must, on the one hand, help the Board of Directors and its members monitor the decisions and, on the other hand, enable the Board of Directors and its members to be accountable to the shareholders and the CSSF. Thus, the routine items may be included succinctly in the minutes of a meeting, in the form of a simple decision, while important items on the agenda involving risks for the institution or jointly discussed must be reported in more detail, allowing readers to follow the discussions and to identify the positions taken.

26. The Board of Directors shall assess the procedures governing its operating mode and its work in order to regularly improve them to ensure their effectiveness and to verify whether the applicable procedures are complied with in practice. It shall ensure that all its members have a clear picture of their obligations, responsibilities and allocation of tasks within the Board of Directors and specialised committees that depend on it.

27. The chairperson of the Board of Directors shall ensure a balanced composition thereof, in particular in terms of diversity, to ensure its proper functioning, to promote a culture of informed discussion in which all parties are heard within the Board of Directors and to propose the appointment of independent directors. The chairperson of the Board of Directors shall not exercise executive functions within the institution. Thus, the mandates of authorised manager and chairperson of the Board of Directors cannot be combined and the chairperson of the Board of Directors cannot be another staff member of the institution.

Section 4.1.4. Specialised committees

28. The Board of Directors may be assisted by specialised committees, in particular, in the fields of audit, risks, compliance, remuneration and appointments or internal governance and professional ethics, according to its needs and considering the organisation, nature, scale and complexity of the institution's activities. The missions of the specialised committees shall be to provide the Board of Directors with critical assessments in respect of the organisation and functioning of the institution in their specific areas of competence.

29. The significant institutions must put in place an audit committee, risk committee, nomination committee and a remuneration committee.

30. In accordance with the principle of proportionality, the institutions that are not significant may put in place dedicated committees combining different areas of responsibility, for example, an audit and risk committee, an audit and compliance committee or a risk and remuneration committee. The members of such committees must possess the necessary knowledge, skills and expertise to perform their functions, both individually and collectively.

31. Without prejudice to the specific legal and regulatory requirements in this respect, the permanent members of the specialised committees shall be, as the case may be, members of the Board of Directors who do not perform any executive function within the institution or independent members. Each committee shall be composed of at least three members whose knowledge, skills and expertise are in line with the missions of the committee. Where there are several specialised committees within an institution and in so far as the number of non-executive and independent members of the Board of Directors allows it, the institution should ensure that the members of the respective committees are different. Moreover, the institution should try to ensure a rotation of the chairpersons and members of the committees, considering the specific experience, knowledge and skills required on an individual and collective basis.

32. The specialised committees shall be chaired by one of their members. These committee chairpersons shall have in-depth knowledge in the area of activities of the committee they chair and shall ensure a critical and constructive debate within the committee.

33. The CSSF recommends that the significant institutions' risk committee have a majority of independent members, including its chairperson.

34. The specialised committees shall meet on a regular basis in order to discharge their tasks and work assigned to them or to prepare the meetings of the Board of Directors. According to their needs, they may be assisted by external experts independent of the institution, and may involve, in their work, the *réviseur d'entreprises agréé*, the authorised managers, the other specialised committees, the heads of the internal control functions and the other persons working for the institution, provided that these persons are not members and do not take part in the recommendations of the committee.

35. The Board of Directors shall lay down, in writing, the missions, composition and working procedures of the specialised committees. Under these procedures, the specialised committees shall receive regular reports from the internal control functions on the development in the institution's risk profile, the breaches of the regulatory framework, the internal governance and the risk management as well as the concerns raised through the internal alert arrangements and the remedial actions. The specialised committees must be able to request any document and information they deem necessary to fulfil their mission. The committees shall document the agendas of their meetings as well as the findings and recommendations according to the same principles as in point 25. Furthermore, the procedures shall provide for the conditions under which the external experts provide their assistance and the terms under which other persons are involved in the work of the specialised committees.

36. The Board of Directors shall ensure that the different committees interact effectively, communicate with each other, with the internal control functions and the *réviseur d'entreprises agréé*, and report to the Board of Directors on a regular basis.

37. The Board of Directors cannot delegate its powers and responsibilities pursuant to this Circular to the specialised committees. Where the Board of Directors is not assisted by specialised committees, the tasks referred to in Sub-sections 4.1.4.1 and 4.1.4.2 shall be directly incumbent upon the Board of Directors.

Sub-section 4.1.4.1. Audit committee

38. The purpose of the audit committee shall be to assist the Board of Directors in the areas of financial information, internal control, including internal audit as well as the audit by the *réviseur d'entreprises agréé*.

39. Without prejudice to the other provisions of Section 4.1.4, the institutions must establish an audit committee when imposed by Article 52 of the Law of 23 July 2016 concerning the audit profession, as amended ("Audit Law").

40. The audit committee shall be in charge of the process of appointment, reappointment, revocation[4] and remuneration of the *réviseur d'entreprises agréé*.

41. The audit committee shall confirm the internal audit charter as well as the multi-annual audit plan and its reviews. It shall assess whether the human and material resources used for the internal audit are sufficient and shall make sure that the internal auditors have the required skills and independence.

[4] *However, the power to appoint the* réviseur d'entreprises agréé *lies with the Board of Directors of the investment firm in accordance with Article 22 of the LFS.*

42. The audit committee shall regularly and critically deliberate on the following[5]:
    - the compliance with the accounting rules and the financial reporting process;
    - the state of the internal control and the compliance with the rules set in this respect in this Circular, in particular, on the basis of the internal audit function reports;
    - the quality of the work carried out by the internal audit function and the compliance with the rules set in this respect;
    - the quality of the work carried out by the *réviseur d'entreprises agréé*, his/her independence and objectivity, his/her compliance with the applicable rules of professional ethics as well as the scope and frequency of the audits. In this respect, the audit committee shall analyse and assess the reports on the annual accounts, the management letters, the long form reports and, where relevant, the appropriateness of the services other than those related to the audit of accounts that have been provided by the *réviseur d'entreprises agréé*;
    - the appropriate and timely follow-up by the authorised management of the recommendations of the internal audit function and the *réviseur d'entreprises agréé* and the actions taken to address the identified problems, shortcomings and irregularities.
43. When reporting to the Board of Directors as a whole, the audit committee shall propose the necessary measures to promptly address the identified problems, shortcomings and irregularities. The audit committee shall inform the Board of Directors of the conclusions of the external audit, of its work to ensure the integrity of the legal reporting and of its role in this process.

Sub-section 4.1.4.2. Risk committee

44. The purpose of the risk committee shall be to advise the Board of Directors on aspects related to the overall risk and risk appetite strategy and also to assist it in assessing the correlation between the incurred risks, the institution's ability to manage these risks, and the internal and regulatory capital and liquidity reserves.

45. The significant institutions must establish a risk committee in accordance with the provisions of Article 7 of RCSSF 15-02.

[5] *Annex 2 of the BCBS guidelines on the internal audit function dated 28 June 2012 ("The internal audit function in banks") includes a more comprehensive list of tasks generally assigned to the audit committee.*

46. The risk committee shall confirm the specific policies of the authorised management in accordance with Section 1.1.2 of Part III. It shall assist the Board of Directors in its supervisory mission, i.e. implementing the risk strategy, the overall risk-taking and risk management framework and the adequacy of all the incurred risks relating to the strategy, the risk appetite and the risk mitigation measures of the institution.

47. The risk committee shall assess whether the human and material resources, as well as the organisation of the risk control function are sufficient and shall ensure that the members of the risk control function have the required skills.

48. The risk committee shall advise and assist the Board of Directors in the recruitment of external experts that the Board of Directors would hire to provide advice or support.

49. The risk committee shall regularly and critically deliberate on the following:
    - the risk profile of the institution, its development as a result of internal and external events, its adequacy in relation to the approved risk strategy, the risk appetite, the policies and the risk limit systems and the ability of the institution to manage and bear these risks on an ongoing basis, considering its internal and regulatory capital and liquidity reserves;
    - the adequacy of the risk-taking and risk management framework in relation to the strategy and the business objectives, the corporate culture and the framework of the institution's values;
    - the quality of the work carried out by the risk control function and the compliance with the rules laid down in this respect in this Circular;
    - the assessment, through stress scenarios and stress testing, of the impact of external and internal events on the risk profile of the institution and the ability of the institution to bear its risks;
    - the appropriate and timely follow-up by the authorised management of the recommendations of the risk control function and the actions taken to address the identified problems, shortcomings and irregularities;
    - the compliance and the pricing of the products and services offered to customers with the business model and the approved risk strategy;
    - without prejudice to the responsibilities of the remuneration committee, the appropriateness of the benefits provided for in the remuneration policies and practices, considering the risk level of the institution, its internal and regulatory capital and liquidity reserves as well as its profitability.

    The risk committee shall report the outcome of its deliberations to the Board of Directors as a whole, by proposing the necessary measures to promptly address the identified problems, shortcomings and irregularities.

50. The chairperson of the risk committee cannot be, at the same time, the chairperson of the Board of Directors or of any other specialised committee.

Sub-chapter 4.2. Authorised management

Section 4.2.1. Responsibilities of the authorised management

51. The authorised management shall be in charge of the effective, sound and prudent day-to-day management of the activities (and inherent risks). This management shall be exercised in compliance with the strategies and guiding principles approved by the Board of Directors and the applicable regulations, by considering and safeguarding the institution's long-term financial interests, solvency and liquidity situation. The authorised management shall constructively and critically assess all the proposals, explanations and information submitted to it for decision. The authorised management shall document its decisions by way of minutes of meetings, which must, on the one hand, help it monitor the decisions and, on the other hand, enable it to account for its management to the Board of Directors and the CSSF. Thus, the routine items may be included succinctly in the minutes of a meeting, in the form of a simple decision, while important items on the agenda involving risks for the institution or jointly discussed must be reported in more detail, allowing readers to follow the discussions and to identify the positions taken.

52. Pursuant to Article 19(2) of the LFS, the members of the authorised management must be authorised to determine the business direction effectively. Consequently, where management decisions are taken by larger management committees rather than solely by the authorised management, at least one member of the authorised management must be part of it and have a veto right.

53. The authorised management must, in principle, be permanently on site. Any exemption to this principle must be authorised by the CSSF.

54. The authorised management shall implement, through written internal policies and procedures, all the strategies and guiding principles laid down by the Board of Directors in relation to central administration and internal governance, in compliance with the legal and regulatory provisions and after having heard the internal control functions. The policies shall include detailed measures to be implemented; the procedures shall be the work instructions which govern this implementation. The term "procedures" is to be taken in the broad sense, including all the measures, instructions and rules governing the organisation and internal functioning.

The authorised management shall ensure that the institution has the necessary internal control mechanisms, technical infrastructures and human resources to ensure a sound and prudent management of the activities (and inherent risks) within the context of robust internal governance arrangements pursuant to this Circular.

55. Under the guiding principles of professional conduct, corporate values and management of conflicts of interest laid down by the Board of Directors, the authorised management shall define an internal code of conduct applicable to all the persons working in the institution. It shall ensure its proper application on the basis of regular controls carried out by the compliance and internal audit functions.

    The purpose of this code of conduct must be the prevention of operational and reputational risks which the institution may incur as a result of administrative or criminal sanctions, restrictive measures imposed on it or legal disputes, the damage to its corporate image or the loss of the trust of its customers and the consumers. The code of conduct should remind the staff, the authorised managers and the members of the Board of Directors of the compliance with the applicable regulations, the internal rules and limitations, the principles that underlie honesty and integrity in their behaviour as well as the cases of inappropriate conduct and the sanction measures arising therefrom.

56. The authorised management must have a full understanding of the organisational and operational structure of the institution, in particular, of the underlying legal entities (structures), of their raison d'être, the intra-group links and interactions as well as the related risks. It shall ensure that the required management information is available, in due time, at all decision-making and control levels of the institution and legal structures which are part of it.

57. In its day-to-day management, the authorised management shall consider the advice and opinions provided by the internal control functions.

    Where the decisions taken by the authorised management have or could have a significant impact on the risk profile of the institution, the authorised management shall first obtain the opinion of the risk control function and of the compliance function.

The authorised management shall promptly and effectively implement the corrective measures to address the weaknesses (problems, shortcomings, irregularities or concerns) identified by the internal control functions, the *réviseur d'entreprises agréé* or through the internal alert arrangements, by considering the recommendations issued in this respect. This approach shall be laid down in a written procedure which the Board of Directors shall approve upon proposal of the internal control functions. According to this procedure, the internal control functions shall prioritise the various weaknesses they identified and set, upon approval of the authorised management, the (short) deadlines by which these weaknesses shall be remedied. The authorised management shall designate the business units or persons in charge of the implementation of the corrective measures by allocating the resources (budget, human resources and technical infrastructure) required for that purpose. The internal control functions shall be in charge of following up on the implementation of the corrective measures. Any significant delay in the implementation of the corrective measures shall be notified by the authorised management to the Board of Directors which must authorise time extensions for the implementation of these measures.

The institution shall establish a similar procedure, approved by the Board of Directors, which shall apply where the CSSF requests the institution to take (corrective) measures. In this case, any significant delay in the implementation of these measures is to be notified by the authorised management to the Board of Directors and the CSSF.

58. The authorised management shall verify the implementation of and compliance with internal policies and procedures. Any breach of internal policies and procedures shall result in prompt and adapted corrective measures.

59. The authorised management shall verify the robustness of the central administration and internal governance arrangements on a regular basis. It shall adapt the internal policies and procedures in light of the internal and external, current and anticipated changes and the lessons learnt from the past.

60. The authorised management shall inform the internal control functions of any major change in the activities or organisation in order to enable them to identify and assess the risks which may arise therefrom.

61. The authorised management shall regularly or at least annually inform the Board of Directors, in a comprehensive manner and in writing, of the implementation, adequacy, effectiveness of and compliance with the internal governance arrangements, comprising the state of compliance (including the concerns raised through the internal alert arrangements) and of internal control as well as the ICAAP/ILAAP reports on the situation and the management of risks, internal and regulatory capital and liquidity reserves.

62. Once a year, the authorised management shall confirm compliance with this Circular to the CSSF by way of a single written sentence followed by the signatures of all the members of the authorised management. Where, due to non-compliance, the authorised management is not able to confirm full compliance with the Circular, the aforementioned statement takes the form of a reservation which outlines the non-compliant items by providing explanations on their raison d'être.

63. Where the authorised management becomes aware that the central administration and internal governance arrangements no longer enable a sound and prudent management of the activities or that the incurred risks are or will no longer be properly borne by the institution's ability to manage these risks, by the internal and regulatory capital and liquidity reserves, it shall inform the Board of Directors and the CSSF by providing them, without delay, with any necessary information to assess the situation.

64. Notwithstanding the joint responsibility of the members of the authorised management, it shall designate at least one of its members who shall be in charge of the administrative, accounting and IT organisation and who shall assume responsibility for implementing the policy and rules that it has established in this context. This member shall be in charge, in particular, of drawing up the organisation chart and the task description which s/he submits, prior to their implementation, to the authorised management for approval. S/he then shall ensure their proper application. The member in question shall also be in charge of the production and publication of accounting information intended for third parties and the transmission of periodic information to the CSSF. Thus, s/he shall ensure that the form and content of this information comply with the legal rules and instructions of the CSSF in this field.

    The authorised management shall also designate, among its members, the person(s) in charge of the internal control functions.

65. The institutions shall inform the CSSF of the appointments and removals of the members of the authorised management, in accordance with the provisions of this Circular and the Prudential Procedure, stating moreover the reasons for the removal.

Section 4.2.2. Qualification of the authorised management

66. The members of the authorised management shall, both individually and collectively, have the necessary professional qualifications (appropriate knowledge, skills and experience), the professional repute and personal qualities to manage the institution and determine the business direction effectively. The personal qualities shall be those which enable them to effectively perform their authorised manager's mandate with the required commitment, availability, objectivity, critical thinking and independence of mind.

Commission de Surveillance du Secteur Financier

Chapter 5. Administrative, accounting and IT organisation

Sub-chapter 5.1. Organisation chart and human resources

67. The institution shall have a sufficient number of human resources on site with appropriate individual and collective professional skills in order to take decisions under the policies laid down by the authorised management and based on delegated powers, and in order to implement the decisions taken in compliance with the existing procedures and regulations. The organisation chart and the task description shall be laid down in writing and made available to all relevant staff in an easily accessible manner.

68. The structure of the different functions (business, support and control) and of the different business units must be presented in the organisation chart, along with the reporting and functional lines with each other and with the authorised management and the Board of Directors.

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

70. The organisation chart and the 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 making them incompatible for the same person. The goal pursued shall be to avoid conflicts of interest and to prevent, through reciprocal control environment, a person from making mistakes and irregularities which would not be identified.

71. Pursuant to Article 19(2) of the LFS, the authorised management shall be jointly liable for the management of the institution. The principle of segregation of duties shall not derogate from this joint liability. It shall remain compatible with the practice whereby the members of the authorised management share the day-to-day tasks relating to the close monitoring of the various activities. The institution must organise this allocation so as to avoid conflicts of interest. Thus, the same member of the authorised management cannot be in charge of or be responsible for functions relating to both the risk-taking and the independent control of these risks. Similarly, the authorised manager who himself/herself serves as Chief Risk Officer and/or Chief Compliance Officer pursuant to point 134 and/or point 148 of this part, cannot, at the same time, be in charge of the internal audit function (cf. incompatibility of functions in the box below). Where, due to the small size of the institution, several duties and responsibilities have to be assigned to the same person, this grouping must be organised so that it does not prejudice the objective pursued by the segregation of duties.

Incompatibility of functions:

The authorised manager, who himself/herself serves as Chief Compliance Officer and/or Chief Risk Officer, irrespective of the fact that s/he is the member of the authorised management in charge of the compliance function and/or the member of the authorised management in charge of the risk control function, cannot, at the same time, be the member of the management body in charge of the internal audit function and/or the Chief Internal Auditor.

72. The institution shall have a continuing vocational training programme which shall ensure that the staff members, the Board of Directors and the authorised management remain qualified and understand the internal governance arrangements as well as their own roles and responsibilities in this regard.

73. Each staff member must take at least two consecutive calendar weeks of personal leave annually. It must be assured that each staff member is actually absent during that leave and that his/her substitute actually takes charge of the work of the absent person.

Sub-chapter 5.2. Procedures and internal documentation

74. The institutions shall document all central administration and internal governance arrangements in writing.

    This documentation shall relate to the strategies, guiding principles, policies and procedures relating to central administration and internal governance. It shall include a clear, comprehensive, detailed and accessible manual of procedures, whose procedures shall be known by the entire staff concerned and which is updated on an ongoing basis.

75. The description of the procedures to ensure the proper execution of activities shall concern the following points:

    - the successive and logical stages of the transaction processing, from initiation to documentation storage (workflow);
    - the controls to be carried out, as well as the means to ensure that they have been carried out.

76. The institutions shall document, in writing, all their transactions, i.e. any process which includes a commitment on the part of the institution as well as the decisions relating thereto. The documentation must 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.

77. The files, working papers and control reports of the internal control functions, experts and service providers referred to in Sub-chapter 6.2 of this part as well as the long form reports drawn up by the *réviseur d'entreprises agréé* shall be kept in the Luxembourg institution during at least five years, without prejudice to other applicable laws, in order to enable the institution to retrace the controls carried out, the identified problems, shortcomings or irregularities as well as the recommendations and conclusions. The CSSF as well as the *réviseur d'entreprises agréé* must always be able to access these documents.

78. All transaction orders initiated by the institution and all correspondence with the customers or their proxies shall be issued by the institution; all correspondence shall be addressed thereto. In the case where the institution has a branch abroad, the latter is the contact point for its own customers.

Sub-chapter 5.3. Administrative and technical infrastructure

79. The institution shall have the necessary and sufficient support functions, material and technical resources to execute its activities.

Section 5.3.1. Administrative infrastructure of the business functions

80. Each business function must be based on an administrative infrastructure which guarantees the implementation of the business decisions and their proper execution, as well as compliance with the powers and procedures for the area in question.

Section 5.3.2. Financial and accounting function

81. The institution shall have a financial and accounting department whose mission is to assume the accounting and financial management of the institution. Some parts of the financial and accounting function within the institution may be decentralised, provided however that the central financial and accounting department centralises and controls all the entries made by the various departments and prepares the global accounts. The financial and accounting department must 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 information to be provided to the CSSF.

    In the significant institutions, the CFO shall be selected, appointed and removed from office according to a written internal procedure and with the prior approval of the Board of Directors.

    The operational tasks linked to the financial and accounting function may be outsourced. This outsourcing of operational tasks shall not result in the transfer of the financial and accounting function as a whole to the service provider.

82. The institution wishing, in accordance with the principle of proportionality, to outsource operational tasks of the financial and accounting function must submit a prior notification to the CSSF, in accordance with the provisions of points 59 and 60 of Circular CSSF 22/806 on outsourcing arrangements. The notification shall include:
    - the analysis and its conclusions justifying the outsourcing of the operational tasks of the financial and accounting function;
    - the decision of the Board of Directors approving the analysis and its conclusions;
    - a description of the outsourcing, the provider chosen, the contracted external resources; and
    - the person in charge of this outsourcing within the institution.

    Outsourcing of the operational tasks linked to the financial and accounting function must be made in compliance with the provisions of Circular CSSF 22/806 on outsourcing arrangements.

83. The financial and accounting function shall operate based on written procedures which shall provide for:
    - the identification and recording of all transactions undertaken by the institution;
    - the explanation of 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;
    - the preparation of the accounts by applying the accounting and valuation rules laid down in the relevant accounting laws and regulations;
    - the verification of the reliability and relevance of the market prices and fair values used while preparing the accounts and of the reporting to the CSSF;
    - the production and transmission of periodic information, including, primarily, the legal and regulatory reporting, to the CSSF, ensuring the information is reliable, particularly in terms of solvency, liquidity, non-performing loan exposures, restructured credits and large exposures;
    - the record-keeping of all accounting documents in accordance with the applicable legal provisions;
    - the drawing-up of, where appropriate, accounts according to the accounting scheme applicable in the home country of the shareholder in order to prepare consolidated accounts;
    - the completion of reconciliation of accounts and accounting entries;

- the production of accurate, complete, relevant, understandable management information available without delay which shall enable the authorised management to take informed decisions and to closely monitor the developments in the financial situation of the institution and its compliance with budget data. This information shall be used as a management control tool and will be more effective if it is based on analytical accounting;
- the guarantee that the financial reporting is reliable.

84. The institutions shall have a management control which is attached either to the financial and accounting department or, in the organisation chart, directly to the authorised management of the institution.

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

86. In connection with the opening of third-party accounts (balance sheet and off-balance sheet), each institution shall define specific rules on the recording of accounts in its accounting system. Moreover, it shall specify the conditions for opening, closing and operating these accounts.

    The institution must avoid having, in its accounting system, a multitude of accounts with uncontrollable items that could lead to the execution of unauthorised 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.

87. The opening and closing of internal accounts in the accounting system must be validated by the financial and accounting department. In case of opening of accounts, this validation must take place before these accounts become operational. The institution shall set out rules concerning the use of such accounts and the powers relating to their opening and closing. The financial and accounting department shall ensure that the internal accounts are periodically subject to a procedure which justifies their need.

    It is necessary to ensure that internal accounts and payable-through accounts are not kept open where they would no longer be in line with the use defined by the set rules.

88. Entries that have a retroactive effect can only be used for regulating purposes.

    Entries that have a retroactive effect as well as entries regarding reversals are to be authorised and supervised by both the departments which are at the origin of these entries and the financial and accounting department.

89. The entire accounting organisation and procedures shall be described in a manual of accounting procedures.

While defining and implementing these procedures, the institutions shall ensure compliance with the principle of integrity in order to avoid, in particular, that the accounting system is used for fraudulent purposes.

Section 5.3.3. IT function

90. The institutions shall organise their IT function so as to have control over it and to ensure robustness, effectiveness, consistency and integrity pursuant to Chapter 3 of this part. For those purposes, they shall comply with the requirements of Circular CSSF 20/750 on requirements regarding information and communication technology (ICT) and security risk management.

91. The institutions which rely on service providers as regards the IT function, shall comply, in particular, with the conditions laid down in Circular CSSF 22/806 on outsourcing arrangements.

Section 5.3.4. Communication and internal and external alert arrangements

92. The internal communication arrangements shall ensure that the strategies, policies and procedures of the institution as well as the decisions and measures taken by the Board of Directors and authorised management, directly or by way of delegation, are communicated in a clear and comprehensive manner to all staff members of the institution, considering their information needs and their responsibilities within the institution. The internal communication arrangements shall enable staff to have easy and constant access to this information.

93. The management information system shall ensure that all management information is, in normal circumstances and in times of stress, transmitted, in a clear and comprehensive manner, and without delay, to all members of the Board of Directors, the authorised management and the staff of the institution, considering their information needs, their responsibilities within the institution and the objective to ensure a sound and prudent business management.

94. The institutions shall maintain internal alert arrangements (whistleblowing) which shall enable the entire staff of the institution to draw attention to legitimate concerns about internal governance or internal and regulatory requirements in general. These arrangements shall respect the confidentiality and identity of the persons who raise such concerns and provide for the possibility to raise these concerns outside the established reporting lines as well as within the Board of Directors. The alerts issued in good faith shall not result in any liability or adverse impact of any sort for the persons who issued them.

95. The CSSF has also made a tool and a procedure to report incidents directly to it available on its website. (https://whistleblowing.apps.cssf.lu/index.html?language=fr).

Section 5.3.5. Crisis management arrangements

96. The crisis management arrangements shall be based on resources (human resources, administrative and technical infrastructure and documentation) which shall be easily accessible and available in emergencies.

97. The crisis management arrangements shall include, where applicable, a recovery plan which shall comply with the requirements of Chapter 2 of Part IV of the LFS.

98. The crisis management arrangements shall be tested and updated, on a regular basis, in order to ensure and maintain its effectiveness.

Chapter 6. Internal control

99. The internal control shall be a control system composed of rules and procedures which aim to ensure that the objectives set by the institution are reached, the resources are effectively used, the risks are controlled and the assets and liabilities are protected, the financial and management information is accurate, comprehensive, relevant, understandable and available without delay, the laws and regulations as well as the internal policies and procedures are complied with and that the requests and requirements of the CSSF are met[6].

100. The internal control arrangements of an institution must be adapted to its organisation and to the nature, scale and complexity of its activities and relating risks and comply with the principles of the "three lines of defence" model.

The first line of defence consists of the business units which take or are exposed to risks, which are responsible for their management and which monitor compliance with the policies, procedures and limits imposed on them, on a permanent basis.

The second line consists of support functions, such as the financial and accounting function, and especially the compliance and the risk control functions which control risks on an independent basis and support the business units in complying with the applicable policies and procedures.

[6] *The internal control mechanisms also provide for mechanisms aimed to prevent execution errors and frauds and to enable their early detection. Pursuant to the principle of proportionality, the institutions whose asset management activity and service activities related, in particular, to the administration of UCIs are significant, shall define adequate internal control mechanisms for these activities, especially in the field of discretionary management, processing of held mails, bookkeeping and net asset value calculation of investment funds.*

The third line consists of the internal audit function which makes an independent, objective and critical assessment of the first two lines of defence and of the internal governance arrangements as a whole.

The three lines of defence are complementary, each line of defence assuming its control responsibilities regardless of the other lines.

The implementation of sound internal control arrangements shall go hand in hand with a relevant segregation of functions, duties and responsibilities, the implementation of a management of information access and the physical separation of certain functions and departments in order to secure data and transactions.

Sub-chapter 6.1. Operational controls

A sound internal control environment shall include the following types of controls:

Section 6.1.1. Day-to-day controls carried out by the operating staff

101. The internal control procedures shall provide that the operating staff control, on a day-to-day basis, the transactions they carry out in order to identify as soon as possible the errors and omissions that occurred during the processing of the current transactions. Examples of these controls are: the verification of the cash account balance, the verification of his/her positions by the trader, the follow-up of outstanding issues by each staff member.

Section 6.1.2. Ongoing critical controls

102. This category of controls shall include inter alia:

- hierarchical control;
- validation (for example dual signature, codes of access to specific features) associated with the monitoring of compliance with the authorisation procedure and procedure for delegating powers adopted by the authorised management;
- reciprocal controls;
- regular statement of the existence and the value of the assets and liabilities, in particular by means of verification of the inventories;
- reconciliation and confirmation of accounts;
- monitoring of the accuracy and completeness of the data transmitted by the heads of the business and operational functions with a view to an administrative follow-up of transactions;
- monitoring of the compliance with the internal limits imposed by the authorised management;

- normal nature of the concluded transactions, in particular, in respect of their price, their scale, the possible guarantees to be received or provided, the profits generated and losses incurred, the amount of possible brokerage fees.

The proper functioning of ongoing critical controls is guaranteed only if the principle of segregation of duties is complied with.

Section 6.1.3. Controls carried out by the members of the authorised management on the activities or functions which fall under their direct responsibility

103. The members of the authorised management shall personally oversee the activities and functions, which fall under their direct responsibility, on a regular basis. These controls shall be carried out based on the data received in this respect from the business, support and control functions or the various business units of the institution.

The areas requiring particular attention by the members of the authorised management are inter alia:

- the risks associated with the activities and functions for which they are directly responsible;
- the compliance with the laws and standards applicable to the institution, with a particular emphasis on prudential standards on solvency, liquidity and regulations on large exposures;
- the compliance with the policies and procedures established by the authorised management;
- the compliance with established budgets: review of actual achievements and gaps;
- the compliance with limits (in particular based on exception reports);
- the characteristics of the transactions, in particular their price, their individual profitability;
- the development of the overall profitability of an activity.

The members of the authorised management shall inform the other members of the authorised management about the exercise of their control function, on a regular basis.

Sub-chapter 6.2. Internal control functions

104. The policies implemented with respect to risk control, compliance and internal audit shall provide for three distinct internal control functions: on the one hand, the risk control function and the compliance function which are part of the second line of defence and on the other hand, the internal audit function which is part of the third line of defence. Moreover, these policies shall describe the fields of intervention directly related to each internal control function, clearly define the responsibilities for the common fields of intervention in order to avoid redundancies and conflicts of powers, and define the objectives as well as the independence, authority, objectivity and permanence of the internal control functions.

Section 6.2.1. General responsibilities of the internal control functions

105. The main purpose of the internal control functions shall be to verify compliance with all the internal policies and procedures which fall within the area for which they are responsible, to regularly assess their adequacy with respect to the organisational and operational structure, the strategies, the activities and the risks of the institution as well as with respect to the applicable legal and regulatory requirements, and to report directly to the authorised management as well as to the Board of Directors and, where appropriate, to the specialised committees. They shall provide the authorised management and the Board of Directors, and, where appropriate, the specialised committees with the opinions and advice they deem useful or which are requested by these bodies or committees.

106. Where they consider that the effective, sound or prudent business management is compromised, the heads of the internal control functions shall promptly inform, on their own initiative, the authorised management and the Board of Directors or, where appropriate, the specialised committees.

107. Where the institution is the group head, its internal control functions shall supervise and control the internal control functions of the different entities of the group. The internal control functions of the institution shall ensure that the problems, shortcomings, irregularities and risks identified throughout the whole group are reported to the local management and supervisory bodies as well as to the authorised management and to the Board of Directors of the group head.

Section 6.2.2. Characteristics of the internal control functions

108. The internal control functions shall be permanent and independent functions each with sufficient authority. The heads of these functions shall have direct access right to the Board of Directors or its chairperson or, where appropriate, to the specialised committees, to the *réviseur d'entreprises agréé* of the institution as well as to the CSSF.

The independence of the internal control functions is incompatible where:

- the staff of the internal control functions are in charge of tasks they are called upon to control;
- the remuneration of the staff of the internal control functions is linked to the performance of the activities they control or is determined according to other criteria which compromise the objectivity of the work carried out by the internal control functions;
- the internal control functions are, from an organisational point of view, included in the business units they control or report hierarchically to them;
- the heads of the internal control functions are subordinated to the persons in charge of, or responsible for, the activities which the internal control functions are called upon to control.

109. The authority which the internal control functions must have, requires that these functions be able to exercise their responsibilities, on their own initiative, express themselves freely and access all external and internal data and information (in all the institution's business units they control) they deem necessary to fulfil their missions.

110. The internal control functions or third parties acting on behalf of these functions must be objective when carrying out their work.

In order to ensure objectivity, the heads of the internal control functions shall be independent minded: they must not make their own judgement conditional upon that of other persons including, in particular, those controlled and shall ensure to avoid conflicts of interest.

111. The members of the internal control functions must, individually and collectively, possess high professional knowledge, skills and experience in the field of financial activities, especially in their field of responsibility with respect to applicable standards. In accordance with the principle of proportionality, the required skill level shall increase with the organisation of the institution and the nature, scale and complexity of the activities and risks. The individual skill must include the ability to make critical judgements and to be heard by the authorised managers of the institution.

The internal control functions shall update the acquired knowledge and organise ongoing training which is adapted to each of the associates.

In addition to their high professional experience, the heads of the internal control functions, who take on such a position for the first time, shall have the necessary theoretical knowledge.

112. In order to guarantee the execution of the tasks assigned to them, the internal control functions shall have the necessary and sufficient human resources, infrastructure and budget, in keeping with the principle of proportionality. The budget must be sufficiently flexible to reflect an adaptation of the missions of the internal control functions in response to changes in the institution's organisation, the activities and risks or upon the occurrence of specific events.

113. The scope of intervention of the internal control functions shall cover the whole institution within the limits of their respective competences. It shall include non-standard and potentially non-transparent activities.

114. Each institution shall take the necessary measures to ensure that the members of the internal control functions perform their functions with integrity and discretion.

Section 6.2.3. Execution of the internal control functions' work

115. The internal control functions shall document the work carried out in accordance with the assigned responsibilities, in particular in order to allow retracing the interventions as well as the conclusions reached.

116. The internal control functions shall report, in writing, on a regular basis and, if necessary, on an ad hoc basis, to the authorised management and the Board of Directors or, where appropriate, to the specialised committees. These reports shall concern the follow-up to the recommendations, problems, shortcomings and irregularities found in the past as well as the new identified problems, shortcomings and irregularities. Each report shall specify the risks related thereto as well as their severity (measuring the impact) and shall propose corrective measures, as well as in general the position of the persons concerned.

Each internal control function shall prepare, at least once a year, a summary report on its activities and its operation covering all the activities assigned to it. As regards the activities, each summary report shall include a statement of the function's activities carried out since the last report, the main recommendations to the authorised management, the (existing or emerging) problems, the major shortcomings and irregularities found since the last report and the measures taken in this respect as well as the statement of the problems, shortcomings and irregularities identified in the last report but which have not yet been subject to appropriate corrective measures. Finally, the report shall indicate the state of their control area as a whole. As far as operation is concerned, the report shall, in particular, comment on the adequacy of the internal human and technical resources, and the nature and level of reliance on external human and technical resources as well as on any problems which may have occurred in this context. This report shall be submitted for approval to the Board of Directors or the competent specialised committees to ensure its follow-up and that the Board of Directors is informed; it shall be submitted for information to the authorised management.

In case of serious problems, shortcomings and irregularities, the heads of the internal control functions shall immediately inform the authorised management, the chairperson of the Board of Directors and, where appropriate, the chairpersons of the specialised committees. In such cases, the heads of the internal control functions may request to be heard by the specialised committees in a private meeting.

The internal control functions shall verify the effective follow-up of the recommendations relating to the problems, shortcomings and irregularities identified in accordance with the procedure laid down in the third paragraph of point 57 of this part. They shall report on this subject to the authorised management on a regular basis.

Section 6.2.4. Organisation of the internal control functions

117. Each internal control function shall be under the responsibility of a separate head of the function who shall be selected, appointed and dismissed in accordance with a written internal procedure. The appointments and removals of the heads of the internal control functions shall be approved beforehand by the Board of Directors and reported in writing to the CSSF in accordance with the Prudential Procedure as published by the CSSF on its website.

118. The heads of the three internal control functions shall be responsible vis-à-vis the authorised management and, ultimately, vis-à-vis the Board of Directors for the performance of their mandate. In this respect, these heads must be able to contact, directly and on their own initiative, the chairperson of the Board of Directors or, where appropriate, the competent specialised committee.

The heads of the three internal control functions shall be referred to as Chief Risk Officer for the risk control function, Chief Compliance Officer for the compliance function and as Chief Internal Auditor for the internal audit function.

Outsourcing of the compliance function and risk control function is not authorised. However, certain ancillary operational tasks in relation to the risk control and compliance function may be outsourced.

The operational tasks of the internal audit function may be outsourced by small institutions with a low and non-complex risk profile. Such outsourcing is not, in principle, acceptable for institutions with agencies, branches or subsidiaries. The Board of Directors of the institution shall remain ultimately responsible for outsourcing the internal audit operational tasks. External providers entrusted with the outsourced internal audit operational tasks shall depend on and report directly to the member of the authorised management in charge of internal audit. They shall also have direct access to the Board of Directors or, where appropriate, the chairperson of the audit committee.

Any outsourcing of the operational tasks linked to the internal control function must be made in compliance with the provisions of Circular CSSF 22/806 on outsourcing arrangements.

119. The provisions of the preceding point shall not exclude the possibility for the internal control functions to use the expertise and human or technical means of third parties (belonging or not to the same group as the institution) for certain aspects. This use shall be governed by an internal procedure which must allow, in particular, the authorised management and the Board of Directors to assess the dependencies and risks which a significant use of these external resources might pose for the institution.

The authorised management shall select these external resources based on an analysis of correlation between the institution's needs and services, the level of objectivity and independence, and the specific skills offered by these third parties which must be independent from the institution's *réviseur d'entreprises* (statutory auditor) and *cabinet de révision agréé* (approved audit firm) and from the group to which these parties belong. The Board of Directors shall approve the external resources selected by the authorised management.

120. Any use of external resources must be based on a written mandate. These third parties shall carry out their work in accordance with the regulatory and internal provisions applicable to the internal control function and the area of control in question. They must be placed under the authority of the head of the internal control function covering the controlled area. This head shall supervise the work of these third parties.

121. Where the institution can demonstrate, in accordance with the principle of proportionality, that there is no justification for setting up a distinct risk control function and compliance function or for appointing two heads of these functions full time, the institution may either set up a combined function or a position with combined responsibility or entrust two different persons with these functions on a part-time basis, subject to prior approval of the CSSF.

The institution wishing to create a combined risk control and compliance function, allocate the responsibilities for these two functions to one single person, combine one of these responsibilities with other tasks or entrust two different persons with these functions on a part-time basis, must submit a request to the CSSF which shall include:

- either a description of the combined function or of the position with combined responsibility, or a description of the functions of the two persons in charge on a part-time basis;
- a description of all the other tasks performed by the person(s) in question;
- the analysis of its conclusions justifying either the creation of a combined function or a position with combined responsibility or the fact of entrusting two different persons with the functions on a part-time basis, given the institution's organisation, the nature, scale and complexity of its activities and risks;
- the decision of the Board of Directors approving the analysis and its conclusions; and
- a written confirmation that the tasks performed by the person(s) in question remain compatible with the aforementioned responsibilities.

122. The institution wishing, in accordance with the principle of proportionality, to outsource the operational tasks of the internal control functions must submit a prior notification to the CSSF, in accordance with the provisions of points 59 and 60 of Circular CSSF 22/806 on outsourcing arrangements. The notification shall include[7]:

- the analysis and its conclusions justifying the outsourcing of the operational tasks of the internal control function;
- the decision of the Board of Directors approving the analysis and its conclusions;
- a description of the outsourcing, the provider chosen, the contracted external resources; and
- the person in charge of this outsourcing within the institution.

[7] For the internal audit function, the decision of the board of directors will have to be taken, where applicable, based on the opinion of the audit committee. The notification shall also include the name of the head of the external team fulfilling the internal audit duties.

Where operational tasks of the internal audit function are outsourced, these external providers may be the internal auditors of the group to which the institution belongs. The Board of Directors shall ensure that these resources are sufficient and that they have the necessary experience and skills to cover all the business areas of the institution and the associated risks as well as the required management to ensure high quality audit.

123. The internal control functions of an institution must also be set up at group level, in the legal entities and in the branches composing the group. These constituent parts must each have their own internal control functions, considering the principle of proportionality.

124. Within the branches, the internal control functions shall depend, from a hierarchical and functional point of view, on the control functions of the legal entities to which they belong and report.

Within the subsidiaries, the internal control functions shall depend, from a functional point of view, on the control functions of the group head. The reports drawn up in accordance with the provisions of this Circular shall be submitted not only to the local authorised management and Board of Directors but also, in summarised form, to the internal control functions of the group head institution which shall analyse them and report the items to be noted in accordance with point 115.

Pursuant to the principle of proportionality, the institution which created three permanent and independent internal control functions may decide not to set up individual internal control functions in the legal entities or branches of the group which are limited in size and activities. In this case, the institution shall ensure that its internal control functions carry out regular and frequent controls, including annual on-site inspections of these entities.

Where the institution is a not parent undertaking, it shall seek to obtain a summary of the reports of the internal control functions of the legal entities in question and have them analysed by its own internal control functions. They shall report the major recommendations, main problems, shortcomings and irregularities identified, agreed corrective measures and the effective follow-up of these measures in accordance with point 115.

125. The principles of this Circular shall not exclude that, for Luxembourg institutions, whether or not they are branches or subsidiaries of Luxembourg financial professionals having internal control functions at the level of these professionals, the internal control functions are functionally linked to those of the professional in question.

Section 6.2.5. Risk control function

Sub-section 6.2.5.1. Scope and specific responsibilities of the risk control function

126. The risk control function shall ensure that all business units anticipate, identify, assess, measure, monitor, manage and duly report all the risks to which the institution is or may be exposed. It shall carry out its tasks continuously and without delay. It shall be a central element of the internal governance and organisation of the institution dedicated to limiting risks. It shall inform and advise the Board of Directors and assist the authorised management, propose improvements in the risk management framework and actively participate in the decision-making processes, ensuring that appropriate attention is given to risk considerations. The ultimate responsibility for the decisions regarding risks shall remain, however, with the business units which take the risks and, finally, with the authorised management and Board of Directors. Thus, the term "risk control function" shall not reduce this function to a simple ex-post "control" of the limits.

127. The scope of intervention of the risk control function shall cover the whole institution, including the risks associated with the complexity of the institution's legal structure and the relationships of the institution with related parties.

128. The risk control function shall ensure that the internal risk objectives and limits are robust and compatible with the regulatory framework, the internal strategies and policies, the activities, and the organisational and operational structure of the institution. It shall monitor compliance with these objectives and limits, propose appropriate remedial measures in case of breach, ensure compliance with the escalation procedure in case of significant breach and ensure that the breaches are remedied as soon as possible.

129. The head of the risk control function shall ensure that the authorised management and the Board of Directors receive an independent, comprehensive, objective and relevant overview of the risks to which the institution is or may be exposed. This overview shall include, in particular, an assessment of the correlation between these risks and the own funds and liquidity reserves and the institution's ability to manage these risks in normal times and in times of stress. This assessment shall be based, in particular, on the stress test programme in accordance with Circular CSSF 11/506. It shall also include an assessment of the correlation between the risks incurred and the risk appetite defined by the Board of Directors. The frequency of this communication shall be adapted to the institution's characteristics and needs, in view of its business model, the risks incurred and its organisation.

The summary annual report of the risk control function, a copy of which shall be provided to the CSSF, possibly duplicates elements of the ICAAP and ILAAP report. The risk control function may therefore refer to the ICAAP and ILAAP report in its summary report, provided that it agrees with the descriptions and analyses of risks contained therein. In case of disagreement, the risk control function shall provide its own assessments and conclusions in its summary report.

130. The risk control function shall ensure that the terminology, methodology and technical resources used for the risk anticipation, identification, measurement, reporting, management and control are consistent and effective.

131. The risk control function shall ensure that the risk assessment is based on conservative assumptions and on a range of relevant scenarios, in particular regarding dependencies between risks. Quantitative assessments shall be validated by qualitative assessment methods and expert judgements based on structured and documented analyses.

The risk control function shall inform the authorised management and Board of Directors of the assumptions, limits and possible deficiencies of the applied analyses and models and must regularly compare its ex-ante assessments of the possible risks measured with ex-post materialised risks to improve the accuracy of its assessment methods (back-testing).

132. The risk control function shall strive to anticipate and recognise the risks arising in a changing environment. In this respect, it shall also monitor the implementation of the changes in the activities ("New Product Approval Process") in order to guarantee that the associated risks remain under control.

Sub-section 6.2.5.2. Organisation of the risk control function

133. The institutions shall create a permanent and independent risk control function, considering the principle of proportionality and the criteria governing its application as well as the considerations regarding the organisation of the internal control functions laid down in Section 6.2.4. Where the organisation of an institution, the scale and complexity of its activities or even the incurred risks justify setting up satellite risk control or compliance functions within the business units, the institution must nevertheless set up a central risk control function to which the different satellite functions shall report. This central function shall manage the consolidated overview of risks and ensure compliance with the defined risk strategies and appetite.

134. Subject to specific authorisation by the CSSF, the member of the authorised management designated as directly in charge of the risk control function may take up the position of Chief Risk Officer himself/herself.

135. Within the significant institutions, the head of the risk control function shall be a member of the authorised management who is independent and individually responsible for the risk control function. Where the principle of proportionality does not require such an appointment, another member of the senior management of the institution may assume that function, provided there is no conflict of interest.

136. The head of the risk control function must be able to challenge the decisions of the authorised management. These challenges and the reasons cited must be documented by the institution. Where the institution gives a veto right over the decisions of the authorised management to the Chief Risk Officer, the scope of this right must be decided clearly and in writing, including the escalation process of the Board of Directors.

The decisions which were given a reasoned negative opinion by the Chief Risk Officer should be subject to an enhanced decision-making process.

Section 6.2.6. Compliance function

This Circular comprises the "general guidelines" contained in the ESMA Guidelines on certain aspects of the MiFID compliance function requirements (ESMA/2012/388) and applies them to all the activities of the institution, including the provision of investment services. Where the institutions implement these requirements in relation to investment services within the meaning of the LFS, they shall take into account the "supporting guidelines" set out in ESMA/2012/388.

Sub-section 6.2.6.1. Compliance charter

137. The operational arrangements of the compliance function in terms of objectives, responsibilities and powers shall be laid down in a compliance charter drawn up by the compliance function and approved by the authorised management and ultimately by the Board of Directors.

138. The compliance charter must at least:

- define the position of the compliance function in the organisation chart of the institution while specifying its key characteristics (independence, objectivity, integrity, competences, authority and adequacy of the resources);
- recognise the compliance function's right of initiative to open investigations about all activities of the institution, including those of its branches and subsidiaries in Luxembourg and abroad, and the right to access all documents, materials and minutes of the consultative and decision-making bodies of the institution, to meet all persons working in the institution, to the extent required to fulfil its mission;

- define the responsibilities and reporting lines of the Chief Compliance Officer;
- describe the relationships with the risk control and internal audit functions as well as possible delegation and/or coordination needs;
- define the conditions and circumstances applicable where external experts or service providers are used;
- establish the right for the Chief Compliance Officer to, directly and on his/her own initiative, contact the chairperson of the Board of Directors or, where appropriate, the members of the audit committee or the compliance committee as well as the CSSF.

The content of the compliance charter shall be brought to the attention of all staff members of the institution, including those who work in branches and subsidiaries in Luxembourg and abroad.

139. The compliance charter must be updated as soon as possible in order to take into account the changes in the applicable standards affecting the institution. Any changes must be approved by the authorised management, confirmed by the audit committee or, where appropriate, the compliance committee and ultimately approved by the Board of Directors. They shall be brought to the attention of all staff members.

Sub-section 6.2.6.2. Scope and specific responsibilities of the compliance function

140. The aim of the compliance function is to anticipate, identify, assess, report and monitor the compliance risks of an institution as well as to assist the authorised management in providing the institution with measures to comply with the applicable laws, regulations and standards. The compliance risks may include a variety of risks such as the reputational risk, legal risk, risk of dispute, risk of sanctions, as well as some other operational risk aspects, in connection with all the institution's activities.

These tasks shall be performed on an ongoing basis and without delay.

141. For the purposes of reaching the objectives set, the responsibilities of the compliance function must cover at least the following aspects:

- The compliance function shall identify the standards to which the institution is subject in the exercise of its activities in the various markets and shall keep records of the main rules. These records must be accessible to the relevant staff of the institution;
- The compliance function shall identify the compliance risks to which the institution is exposed in the exercise of its activities and assess their significance and the possible consequences. The compliance risk classification so determined must enable the compliance function to develop a control plan according to the risk, thereby allowing an effective use of the compliance function's resources;

- The compliance function shall ensure the identification and assessment of the compliance risk before the institution expands into new activities, products or business relationships, as well as when developing transactions and the network of a group at international level ("New Product Approval Process");
- The compliance function shall ensure that, for the implementation of the compliance policy, the institution has rules that can be used as guidelines by the staff from different disciplines in the exercise of their day-to-day tasks. These rules must be appropriately reflected in the instructions, procedures and internal controls of areas directly under the compliance function and shall take into account the institution's code of conduct and corporate values;
- The areas falling directly under the remit of the compliance function are typically the fight against money laundering and terrorist financing, the investment services, the prevention regarding market abuse and personal transactions, the frauds, the protection of the customers' interests and data and the prevention and management of conflicts of interest. This list is not exhaustive and each institution shall decide whether its compliance function should also cover compliance with rules other than those listed above;
- The Chief Compliance Officer shall ensure, in particular, that the fight against money laundering and terrorist financing translates into effective controls and measures which are appropriate to the risk. The summary report of the compliance function, a copy of which shall be submitted to the CSSF, shall cover the field of anti-money laundering and counter terrorist financing in a dedicated chapter laying down the activities and events relating to this area, i.e. the main recommendations issued, major (existing or emerging) deficiencies, irregularities and problems identified, the corrective and preventive measures implemented, as well as a list of deficiencies, irregularities and problems which have not yet been subject to appropriate corrective measures;
- In general, the compliance function shall be organised so that it covers all the areas which may result in compliance risks. The areas other than those listed above may not be directly covered by the compliance function. The compliance risk is then to be covered by the other internal control functions in accordance with a compliance policy clearly defining the duties and responsibilities of the different stakeholders in this area and subject to compliance with the segregation of duties. In this case, the Chief Compliance Officer shall assume the role of coordination, centralisation of information and verification that the other areas, which do not directly fall within his/her scope of intervention, are well covered.

142. The compliance function shall verify compliance with the compliance policy and procedures, on a regular basis, and shall be in charge of the adaptation proposals, if required. To this end, the compliance function shall assess and control the compliance risk, on a regular basis, in the context of a structured monitoring programme. In respect of the compliance risk controls and the verification of the procedures and instructions, the provisions of this Circular shall not prevent the compliance function from taking into account the internal audit work.

143. The compliance function shall centralise all information on the compliance problems (inter alia internal and external frauds, breaches of standards, non-compliance with procedures and limits or conflicts of interest) identified by the institution.

In so far as it did not obtain this information as part of its involvement, it shall examine relevant documents, whether internal (for instance control reports and internal audit reports, reports or statements of the authorised management or, where appropriate, the Board of Directors) or external (for instance reports of the *réviseur d'entreprises agréé*, correspondence from the CSSF or other competent authorities).

144. The compliance function shall assist and advise the authorised management on issues of compliance and applicable laws, regulations and standards, notably by drawing its attention to changes in standards which may subsequently have an impact on the compliance area.

145. The compliance function shall raise awareness of the staff about the significance of compliance and related aspects and assist them in their day-to-day operations related to compliance. To this end, it shall also develop an ongoing training programme and ensure its implementation.

146. The Chief Compliance Officer shall be the key contact person of the competent authorities in relation to the fight against money laundering and terrorist financing, for any question in this respect as well as in relation to market abuse. It shall also be in charge of the transmission of any information or report to these authorities.

Sub-section 6.2.6.3. Organisation of the compliance function

147. The institutions shall create a permanent and independent compliance function, considering the principle of proportionality and the criteria governing its application as well as general considerations regarding the organisation of the internal control functions laid down in Section 6.2.4.

148. Subject to specific authorisation by the CSSF, the member of the authorised management designated as directly in charge of the compliance function may take up the position of Chief Compliance Officer himself/herself.

Section 6.2.7. Internal audit function

Sub-section 6.2.7.1. Internal audit charter

149. The operational arrangements of the internal audit function in terms of objectives, responsibilities and powers must be laid down in an internal audit charter drawn up by the internal audit function and approved by the authorised management, confirmed, where appropriate, by the audit committee, and ultimately approved by the Board of Directors.

The internal audit charter must at least:

- define the position of the internal audit function in the organisation chart of the institution while specifying the key characteristics (independence, objectivity, integrity, competence, authority and adequacy of resources);
- confer to the internal audit function the right of initiative and authorise it to review all the activities and functions of the institution including those of its branches and subsidiaries in Luxembourg and abroad as well as the outsourced activities and functions, to access all documents, materials, minutes of the consultative and decision-making bodies of the institution, to meet all persons working in the institution, to the extent required to fulfil its mission;
- lay down the reporting and functional lines of the conclusions that may be drawn from the audit missions;
- define the relationships with the compliance and risk control functions;
- define the conditions and circumstances applicable where third-party experts or service providers are used;
- define the nature of the work and conditions under which the internal audit function may provide internal consulting services or perform other special missions;
- define the responsibilities and reporting lines of the head of the internal audit function;
- establish the right for the Chief Internal Auditor to, directly and on his/her own initiative, contact the chairperson of the Board of Directors or, where appropriate, the members of the audit committee as well as the CSSF;
- specify the recognised professional standards governing the functioning and work of the internal audit[8] ;
- specify the procedures to be observed in respect of coordination and cooperation with the *réviseur d'entreprises agréé*.

[8] *Such as, for example, the International Professional Practices Framework (IPPF) of the Institute of Internal Auditors (IIA).*

The content of the internal audit charter shall be brought to the attention of all staff members of the institution, including those who work in branches and subsidiaries in Luxembourg and abroad.

The internal audit charter must be updated as soon as possible to take into account the changes that have occurred. Any changes must be approved by the authorised management, confirmed, where appropriate, by the audit committee and ultimately approved by the Board of Directors. They shall be brought to the attention of all staff members.

150. The internal audit department shall have a sufficient number of staff and have the required skills as a whole to cover all activities of the institution. The internal auditors must have sufficient knowledge of the audit techniques.

In order not to jeopardise their independence of judgement, the persons from the internal audit cannot be in charge of the preparation and establishment of elements of the central administration and internal governance arrangements. This principle shall not prevent them from taking part in the implementation of sound internal control mechanisms through opinions and recommendations which they provide in this respect. Moreover, in order to avoid conflicts of interest, a rotation of the control tasks assigned to the various internal auditors shall be ensured, where possible, and it should be avoided that the auditors hired within the institution audit the activities or functions which they used to perform themselves recently.

Sub-section 6.2.7.2. Specific responsibilities and scope of the internal audit function

151. The internal audit function shall examine and assess, among others (non-exhaustive list[9]), the following in accordance with the organisation and the nature, scale and complexity of the activities:

- monitoring of compliance with the laws and regulations as well as any prudential requirements imposed by the CSSF;
- effectiveness and efficiency of central administration, governance and internal control arrangements, including the risk control and compliance functions;
- adequacy of the administrative, accounting and IT organisation;
- safeguarding of the values and assets;
- adequacy of the segregation of duties and of the execution of transactions;

[9] *Principle 7 of the document "BCBS_223 The internal audit function in banks" contains a more comprehensive list of activities which may fall within the scope of the institutions' internal audit function.*

- accurate and complete registration of the transactions and the production of accurate, complete, relevant and understandable financial and prudential information available without delay to the Board of Directors and, where appropriate, the specialised committees, to the authorised management and the CSSF;
- implementation of the decisions taken by the authorised management and by the persons acting by delegation and under its responsibility;
- compliance with the policies and procedures, in particular those governing capital adequacy and internal liquidity reserves;
- adequacy of the risk management;
- integrity of the processes ensuring the reliability of the methods and tools used by the institution, the assumptions and data used in the internal models, the qualitative tools for risk identification and assessment, as well as the risk mitigation measures taken;
- operation and effectiveness of the compliance and risk control functions.

152. Where there is, within the institution, a separate department in charge of the control or supervision of a specific activity or function, the existence of such a department shall not discharge the internal audit department from its responsibility to audit this specific area. However, the internal audit department may take into account, in its work, assessments issued by this department on the area in question.

The internal audit must be independent from the other internal control functions which it audits. Consequently, the risk control function or the compliance function cannot be part of the internal audit department of an institution. However, these functions may take into account the internal audit work as regards the verification of the correct implementation of the applicable standards to the exercise of the activities by the institution.

153. The establishment of a local internal audit function in the subsidiaries of the institution shall not discharge the internal audit of the group head from carrying out regular on-site inspections of these local internal audit functions.

Sub-section 6.2.7.3. Execution of the internal audit work

154. All internal audit missions shall be planned and executed in accordance with an internal audit plan. The plan shall be established by the head of the internal audit function for a period of several years (in general three years). Its purpose shall be to cover all activities and functions, considering both the risks posed by an activity or function and the effectiveness of the organisation and internal control in place for this activity or function (risk-based approach). The plan shall consider the opinions issued by the Board of Directors or, where appropriate, the audit committee as well as the authorised management. The plan shall cover all matters of prudential interest (including the CSSF's observations and requests) and shall also reflect the developments and innovations provided for as well as the risks which may arise therefrom.

155. The plan shall be discussed with the authorised management and, where appropriate, with the audit committee and ultimately approved by the Board of Directors. It shall be reviewed, on an annual basis, and adapted to developments and emergencies. The plan shall be reviewed by the authorised management and, where appropriate, by the audit committee before being approved by the Board of Directors. The approval implies that the authorised management provides the internal audit department with the means necessary to implement the internal audit plan.

In its summary report to the Board of Directors, the internal audit shall indicate and state the reasons for the main changes brought to the audit plan as initially approved by the Board of Directors: cancelled missions, delayed missions as well as the missions whose scope has significantly changed.

156. The plan shall set out the objectives of each mission and the scope of the tasks to be executed, give an estimate of the necessary time and human and material resources and assign an audit frequency to each activity and risk.

The internal audit plan shall also provide for the adequate and sufficiently frequent coverage, within a multi-year planning period, of important or complex activities with a potential significant risk, including a reputational risk. It shall focus on the risk of execution errors and the risk of fraud.

The internal audit plan shall provide for adequate coverage of areas with a risk of money laundering or terrorist financing, so that the internal audit may give an account of the compliance with the policy regarding the fight against money laundering or terrorist financing in its summary report on an annual basis.

157. Where the internal audit department of the parent undertaking of the Luxembourg institution carries out on-site inspections of its subsidiary on a regular basis, it is recommended for reasons of effectiveness that, in so far as possible, the Luxembourg institution coordinates its internal audit plan with that of the parent undertaking.

158. The internal audit department shall regularly inform the authorised management and, where appropriate, the audit committee on the implementation of the internal audit plan.

159. Each internal audit mission shall be planned, executed and documented in compliance with the professional standards adopted by the internal audit function in its internal audit charter.

160. Each mission shall be the subject of a written report of the internal audit department intended for the audited persons, the authorised management as well as - possibly in summarised form - for the Board of Directors (and, where appropriate, the audit committee). The reports shall also be made available to the *réviseur d'entreprises agréé* and the CSSF. These reports shall be drafted in French, German or English.

The internal audit department shall prepare a table of the internal audit missions and the written reports related thereto. It shall draft, at least once a year, a summary report.

Sub-section 6.2.7.4. Organisation of the internal audit function

161. The institutions shall create a permanent and independent internal audit function, considering the principle of proportionality and the criteria governing its application as well as the considerations regarding the organisation of the internal control functions laid down in Section 6.2.4.

162. In case the operational tasks of the internal audit function are outsourced, the service providers shall carry out their work under the internal audit plan of the institution by following a work programme, by producing detailed documentation on their work and by drafting reports for each mission. These reports shall be drafted in French, German or English and submitted to the designated head of the function, the management body and, where appropriate, the audit committee. Where these service providers act as *réviseurs d'entreprises agréés*, they must, in all respects, be independent from the *réviseur d'entreprises agréé* and the *cabinet de révision agréé* of the institution as well as from the group to which these persons belong. The provisions of Circular CSSF 22/806 on outsourcing arrangements shall apply.

Chapter 7. Specific requirements

Sub-chapter 7.1. Organisational structure and legal entities (Know-your-structure)

163. The organisational structure shall, in terms of legal entities (structures), be appropriate and justified as regards the strategies and guiding principles. It shall be clear and transparent for all the stakeholders.

The legal, organisational and operational structure must enable and promote effective, sound and prudent business management. It must not impede the sound governance of the institution, in particular the ability of the management body, to effectively manage and oversee the activities (and the risks) of the institution and the different legal entities which are part of it.

The group head institution shall clearly define and delineate the powers which it agrees to delegate to the managers of the legal entities which are part of the group in order to make sure that the parent undertaking can monitor their activity, on an ongoing basis, and that it is involved in any transaction of a certain importance.

164. The guiding principles that the Board of Directors lays down as regards the organisational structure (in terms of legal entities) shall provide notably that:
- the organisational structure is free from any undue complexity;
- the production and distribution, in a timely manner, of all information necessary for a sound and prudent management of the institution and the legal entities which are part of it are ensured;
- any significant flow of management information between legal entities which are part of the institution is documented and may be promptly provided to the Board of Directors, the authorised management, the internal control functions or the CSSF upon their request.

Section 7.1.1. Complex structures and non-standard or potentially non-transparent activities

165. Non-standard or potentially non-transparent activities are those carried out through complex legal entities or arrangements or in jurisdictions which lack transparency or do not meet international standards.

166. The guiding principles regarding internal governance, which the Board of Directors lays down, shall provide, notably that complex structures and non-standard or potentially non-transparent activities are subject to an in-depth analysis and an ongoing monitoring of risks, in particular, those associated with financial crime. Irrespective of the fact that the activities are carried out for own account or for the account of customers, the institution must understand the usefulness of these structures and manage the risks that accompany their establishment and their operational functioning.

Sub-chapter 7.2. Management of conflicts of interest

167. The policy on the management of conflicts of interest shall cover all conflicts of interest, for economic, personal, professional or political purposes, whether they are persistent or linked to a single event. Particular attention must be given to the conflicts of interest between the institution and its related parties and service providers. This policy shall be applicable to all staff as well as to the authorised management and members of the Board of Directors.

168. The policy on the management of conflicts of interest shall provide that all current and possible conflicts of interest must be identified, assessed, managed and mitigated or avoided. Where conflicts of interest remain, the policy in this respect shall lay down the procedures to be followed in order to report, document and manage them so as to avoid that the institution, its counterparties and the customers suffer unjustified consequences thereof. The policy and procedures in question shall also include the procedure to be followed in case of non-compliance with this policy.

169. The policy on the management of conflicts of interest shall provide for the identification of the main sources of conflicts of interest - potentially affected relationships and activities as well as all internal and external parties involved - with which the institution or its staff and its representatives are or may be faced. It shall take into consideration not only present situations and events which may result in conflicts of interest, but also those in the recent past in so far as these events continue to have a potential impact on the institution or person concerned. The institution shall determine the materiality of the identified conflicts and shall decide how they must be managed.

170. In order to minimise the possible conflicts of interests, the institution shall set up an appropriate segregation of duties and activities, including through the management of information access and the use of Chinese walls.

171. The policy on the management of conflicts of interest shall also determine the reporting and escalation procedures applicable within the institution. Where the staff members are or have been faced with a conflict of interest, they shall promptly inform their senior manager on their own initiative. The members of the authorised management and the Board of Directors, who are subject to a conflict of interest, shall promptly inform the authorised management or the Board of Directors, respectively, on their own initiative. The procedures in this regard shall provide that these members shall abstain from participating in decision-making where they may have a conflict of interest or where they are prevented from deciding with full objectivity and independence.[10]

172. The internal control functions shall be in charge of identifying and managing conflicts of interest.

Section 7.2.1. Specific requirements relating to conflicts of interest involving related parties

173. The transactions with related parties shall be subject to the Board of Directors' approval where they have or may have, individually or on an aggregate basis, a significant and negative impact on the risk profile of the institution.

[10] *This provision is in line with those of Articles 441-7 (one-tier system) and 442-18 (two-tier system) of the Law of 10 August 1915 on commercial companies which lays down that any director or member of the supervisory board, respectively, or the member of the Executive Board having an interest in a transaction submitted for approval of the body concerned which conflicts with that of the company, shall inform the body in question thereof and cause a record of his/her statement to be included in the minutes of the meeting. S/he may not take part in these deliberations.*

174. Any material change in significant transactions carried out with related parties must be brought to the attention of the Board of Directors as soon as possible.

175. Transactions with related parties must be carried out in the interest of the institution. The institution's interest is not met where transactions with related parties:

- are carried out on less advantageous terms for the institution than those which would apply to the same transaction carried out with a third party (at arm's length);
- impair the solvency, liquidity situation or risk management abilities of the institution from a regulatory or internal point of view;
- exceed the risk management and control capacities of the institution or are not part of the standard activities of the institution;
- are contrary to the sound and prudent management principles in the interest of the institution.

176. Where the institution is group head, it shall consider, in a balanced way and in compliance with the applicable legal provisions, the interests of all legal entities and branches which are part of the group. It shall consider how these interests contribute to the common objectives and interests of the group over the long term.

Sub-chapter 7.3. New Product Approval Process

177. The new product approval process shall cover the development of new activities in terms of products, services, markets, systems and processes or customers as well as their material changes and exceptional transactions.

It must ensure that any new product remains consistent with the guiding principles established by the Board of Directors, the risk strategy, the risk appetite of the institution and the corresponding limits.

178. The new product approval process shall define, in particular, the changes in the activities subject to the approval process, the considerations to be taken into account, the main issues to be addressed as well as the implementation of the approval process, including the responsibilities of all the parties concerned.

The main issues to be addressed shall include regulatory compliance, accounting, pricing models, the impact on risk profile, capital adequacy and profitability, the availability of adequate front, back and middle office resources and the availability of adequate internal tools and expertise to understand and monitor the associated risks.

179. Consequently, the institutions shall carefully analyse any proposed change in the activities and ensure that they have the ability to bear the risks related thereto, the technical infrastructure and sufficient and competent human resources to control these activities and the associated risks. The business unit requesting the change in its activities shall be in charge of issuing an analysis of the risks in this regard. Similarly, the risk control function shall carry out a prior, objective and comprehensive analysis of the risks associated with any proposed change in the activities. The risk analysis shall take into account the various scenarios and shall indicate, in particular, the ability of the institution to bear, manage and control the risks inherent in the planned activities. The compliance risk inherent in new products shall also be subject to prior analysis by the compliance function.

180. No new activity must be undertaken unless the authorised management approved it, all relevant parties have been heard, and the means mentioned in the preceding point are available.

181. The internal control functions may require that a change in activities shall be deemed to be material and thus be subject to the approval process.

Sub-chapter 7.4. Outsourcing

182. Outsourcing must be compliant with the regulatory requirements of Circular CSSF 22/806 on outsourcing arrangements.

183. The use of outsourcing must not lead to a situation where the spirit or the letter of the applicable legal provisions and of this Circular in terms of central administration, internal governance and risk management are no longer observed.

Chapter 8. Legal reporting

184. The investment firms shall provide the CSSF with the ICAAP/ILAAP reports and the annual certificate of compliance with the requirements of this Circular issued by the authorised management as well as the summary reports of the internal control functions. This information shall be submitted to the CSSF, at the latest, one month after the ordinary general meeting that approved the annual accounts. The relevant information shall be drafted in French, German or English.

Part III. Risk management

Chapter 1. General principles as regards risk measurement and risk management

Sub-chapter 1.1. Institution-wide risk management framework

Section 1.1.1. General information

1. The institutions shall put in place a consistent and exhaustive institution-wide risk management framework, which covers all the activities and operational units of the institutions, including the internal control functions, and which fully recognises the economic substance of all their exposures, allowing the management body to retain control over all the risks to which the institutions are or may be exposed.

2. The risk management framework must include a set of policies and procedures, limits, controls and alerts ensuring the identification, measurement, management or mitigation and report of these risks by the operational units, the institution as a whole, including, if necessary, at consolidated and sub-consolidated levels.

Section 1.1.2. Specific (risk, capital and liquidity) policies

3. The risk policy which implements the risk strategy defined by the Board of Directors shall include:
   - the determination of the institution's risk appetite;

- the definition of a complete and consistent internal limit system which is adapted to the organisational and operational structure, the strategies and policies of the institution and which limits risk-taking in accordance with the institution's risk appetite. This system shall include the risk acceptance policies which define which risks can be taken and the criteria and conditions applicable in this regard;
- the measures aimed to promote a sound risk culture;
- the measures to be implemented in order to ensure that risk-taking and risk management comply with the set policies and limits. These measures shall include, in particular, the existence of a risk control function, alert thresholds and management arrangements for limit breaches, including corrective measures for breaches, a follow-up procedure of the corrective measures as well as an escalation and sanction procedure in the event of continuing breach;
- the definition of a risk management information system;
- the measures to be taken in case of risk materialisation (crisis management and business continuity arrangements).

The risk policy shall describe how the various risks are identified, measured, managed, monitored and reported. It shall lay down the specific approval process which governs risk-taking (and the implementation of possible mitigation measures) as well as the measurement and reporting processes which ensure that the institution has a thorough overview of all the risks at all times.

Pursuant to the provisions of Chapter 2 of Part III of this Circular, the risk policy shall take due account of concentration risks.

4. The capital and liquidity policy implementing the strategy of the Board of Directors in respect of regulatory and internal capital and liquidity shall include, in particular:
   - the definition of internal standards in relation to the management, size and quality of the regulatory and internal capital and liquidity. These internal standards must enable the institution to cover the risks incurred and to have reasonable security margins in case of significant financial losses or liquidity bottlenecks by reference, in particular, to Circular CSSF 11/506;
   - the implementation of sound and effective processes to plan, monitor, report and modify the amount, type and distribution of the regulatory and internal capital and liquidity reserves, in particular in relation to internal capital and liquidity requirements for risk coverage. These processes shall enable the authorised management and the operating staff to have sound, reliable and comprehensive management information as regards risks and their coverage;
   - the measures implemented in order to ensure a permanent adequacy of the regulatory and internal capital and liquidity (reserves);

- the measures taken in order to effectively manage stress situations (capital inadequacy or regulatory or internal liquidity bottleneck);
- the designation of functions in charge of the management, functioning and improvement of the processes, limit systems, procedures and internal controls mentioned in the above indents.

Section 1.1.3. Risk identification, management, measurement and reporting

5. The inherent and residual risks shall be assessed based on an objective and critical analysis specific to the institution. It should not rely solely on external assessments.

6. The institution must explicitly reflect all the different risks in its internal governance arrangements including, in particular, the strategies and policies on risks and on capital and liquidity reserves.

7. The risk management in respect of related parties shall be included in all the elements of the internal governance arrangements.

8. The risk measurement and reporting arrangements shall enable the institution to obtain the required aggregate overviews in order to manage and control all risks of the institution and legal entities (structures) composing it.

9. The decisions on risk-taking and risk strategies and policies shall consider the theoretical and practical limits inherent in the risk models, methods and quantitative risk measures as well as the economic environment in which these risks fall.

10. In general, the risk measurement techniques implemented by an institution shall be based on choices, assumptions and approximations. There is no absolute measurement.

    Consequently, the institutions must avoid any excess of confidence in any specific methodology or model. The risk measurement techniques used must always be the subject of an internal, independent, objective and critical validation and the risk measurements which arise from these techniques are to be critically assessed, and wisely and carefully used by all staff, the authorised management and the Board of Directors of the institution. The quantitative risk assessments shall be supplemented by qualitative approaches, including (independent) expert judgements, based on structured and documented analyses.

Chapter 2. Concentration risk

11. Concentration risk results, in particular, from large concentrated exposures to customers, counterparties or service providers, respectively, groups of customers, counterparties or related service providers, including related parties, to countries or sectors (industries) as well as to specific products or markets (intra-risk concentration). These exposures are not necessarily limited to balance sheet items or off-balance sheet items. Moreover, concentration risk may be the result of various risks (credit risk, market risk, liquidity risk, operational risk - in particular those related to outsourcing - or systemic risk) which combine (inter-risk concentration).

    Intra-risk or inter-risk concentrations may result in economic and financial losses as well as in a significant and negative impact on the risk profile of the institution.

    Concentration risk must be subject to particular vigilance and identification effort as it may jeopardise the financial stability of the institution.

Chapter 3. Risk transfer pricing

12. The institutions shall implement a pricing mechanism for all risks incurred. This mechanism, which is part of the internal governance arrangements, serves as an incentive to effectively allocate the financial resources in accordance with the risk appetite and the principle of sound and prudent business management.

13. The pricing mechanism shall be approved by the authorised management and monitored by the risk control function. The transfer prices must be transparent and communicated to the relevant staff members. The comparability and consistency of the internal transfer pricing systems used within the group must be ensured.

14. The institution shall establish a complete and effective internal transfer pricing system for liquidity. This system shall include all liquidity costs, benefits and risks.

Chapter 4. Wealth management and associated activities ("private banking" activities)

15. Wealth management and its associated activities are especially exposed to money laundering or terrorist financing risks. Consequently, the institutions carrying out these activities shall pay particular attention to comply with the anti-money laundering and counter terrorist financing obligations, whether they are regulatory, deriving from internal policies and procedures or falling within the good practices and organisation recommendations recognised as authority in this field.

16. These institutions shall have sound processes to ensure that the business relationships with their customers comply with the agreements concluded with these customers. This objective may be best achieved when the discretionary management, advice management and simple execution of activities are separated from an organisational point of view.

17. These institutions shall have sound arrangements to ensure compliance with the customers' risk profiles, for the purposes, in particular, of fulfilling the requirements arising from the MiFID regulations.

18. These institutions shall have sound arrangements in place to ensure the communication of accurate information to the customers on the state of their assets. The issue and distribution of account statements and any other information on the state of assets must be separated from the business function.

19. The physical inflows and outflows of cash, securities or other valuables must be carried out and overseen by a function separated from the business function.

20. Any entry and amendment of customers' identification data must be carried out or overseen by a function that is independent from the business function.

21. If a customer purchases a derivative traded on an organised market, the institution shall forthwith pass on (at least) the margin calls to be provided by the institution to the customer.

22. These institutions must have sound arrangements in respect of control of credits (or loans) granted in the context of the provision of ancillary services referred to in point (2) of Section C of Annexe II of the LFS. The financial guarantees covering these credits must be sufficiently diversified and liquid. For the purposes of having an adequate security margin, prudent discounts must be applied according to the nature of the financial guarantees. These institutions must have an early warning system independent from the business function which organises the monitoring of the financial guarantees' value and triggers the liquidation process of the financial guarantees. It must ensure that the liquidation process is triggered in good time, and in any case before the value of the guarantees becomes lower than the credit. Contracts with customers must clearly describe the procedure triggered in the event of inadequacy of the guarantees.

Chapter 5. Exposures to shadow banking entities

23. This chapter shall only apply to institutions to which Part Four (Large exposures) of the CRR applies, in accordance with the level of application set out in Title II of Part One of said regulation.

Sub-chapter 5.1. Implementation of sound internal control principles

24. These institutions shall put in place an internal framework for the identification, management, monitoring and mitigation of the risks arising from the exposures to shadow banking entities[11] in accordance with EBA/GL/2015/20.

25. These institutions shall apply a materiality threshold to identify the exposures to shadow banking entities. In accordance with EBA/GL/2015/20, any individual exposure to a shadow banking entity that is equal to or in excess of 0.25%[12] of the institution's eligible capital[13], after taking into account the effect of the credit risk mitigation and exemptions[14], must be taken into consideration and cannot be deemed as low exposure.

[11] Shadow banking entities are defined in paragraph 11 "Definitions" of EBA/GL/2015/20. These entities are undertakings that carry out one or more credit intermediation activities and that are not excluded undertakings within the meaning of said paragraph. "Credit intermediation activities" shall mean "bank-like activities involving maturity transformation, liquidity transformation, leverage, credit risk transfer or similar activities".

[12] According to the definition "Exposures to shadow banking entities" of paragraph 11 of EBA/GL/2015/20.

[13] Within the meaning of point (71) of Article 4(1) of the CRR.

[14] i) Credit risk mitigating effects in accordance with Articles 399 and 403 of the CRR;

ii) Exemptions provided for in Articles 400 and 493(3) of the CRR.

26. These institutions shall ensure that any possible risks for the institution as a result of their various exposures to shadow banking entities are adequately taken into account within the institution's Internal Capital Adequacy Assessment (ICAAP) and capital planning.

Sub-chapter 5.2. Application of quantitative limits

27. These institutions shall limit their exposures to shadow banking entities in accordance with one of the two approaches (principal approach or fallback approach) as defined in EBA/GL/2015/20.

28. In accordance with the principal approach, these institutions must set an aggregate limit to their exposures to shadow banking entities relative to their eligible capital.

29. When setting an aggregate limit to exposures to shadow banking entities, each of these institutions must take into account:
    - its business model, risk management framework and risk appetite;
    - the size of its current exposures to shadow banking entities relative to its total exposures and relative to its total exposure to regulated financial sector entities;
    - interconnectedness, on the one hand, between shadow banking entities and, on the other hand, between shadow banking entities and the institution.

30. Independently of the aggregate limit, and in addition to it, these institutions must set tighter limits on their individual exposures to shadow banking entities.

31. When setting those limits, as part of their internal assessment process, these institutions must take into account:
    - the regulatory status of the shadow banking entity, in particular whether it is subject to any type of prudential or supervisory requirements;
    - the financial situation of the shadow banking entity including, but not limited to, its capital position, leverage and liquidity position;
    - information available about the portfolio of the shadow banking entity, in particular non-performing loans;
    - available evidence about the adequacy of the credit analysis performed by the shadow banking entity on its portfolio, if applicable;
    - whether the shadow banking entity will be vulnerable to asset price or credit quality volatility;
    - concentration of credit intermediation activities relative to other business activities of the shadow banking entity;
    - interconnectedness, on the one hand, between shadow banking entities and, on the other hand, between shadow banking entities and the institution;

- any other relevant factors identified by the institution as exposures to shadow banking entities, all potential risks to the institution arising from those exposures, and the potential impact of those risks.

32. If these institutions are not able to apply the principal approach as set out above, their aggregate exposures to shadow banking entities must be subject to the limits on large exposures in accordance with Article 395 of the CRR (hereinafter the "fallback approach").

33. The fallback approach must be applied in the following way:
    - If institutions cannot meet the requirements regarding effective processes and control mechanisms or oversight by their management body as set out in Section 4 of EBA/GL/2015/20, they must apply the fallback approach to all their exposures to shadow banking entities (i.e. the sum of all their exposures to shadow banking entities).
    - If institutions can meet the requirements regarding effective processes and control mechanisms or oversight by their management body as set out in Sub-chapter 5.1 of this part, but cannot gather sufficient information to enable them to set out appropriate limits as set out in Sub-chapter 5.2, they must only apply the fallback approach to the exposures to shadow banking entities for which the institutions are not able to gather sufficient information. The principal approach as set out in Sub-chapter 5.2 must be applied to the remaining exposures to shadow banking entities.

Chapter 6. Interest rate risk

Sub-chapter 6.1. Interest rate risk arising from non-trading book activities

34. When implementing Article 14 (Interest rate risk arising from non-trading book activities) of RCSSF 15-02, the CRR investment firms shall comply with the EBA Guidelines on the management of interest rate risk arising from non-trading book activities (EBA /GL/2018/02).

Sub-chapter 6.2. Corrections to modified duration for debt instruments

35. The CRR investment firms applying the standardised approach for the calculation of their capital requirements associated with the general interest rate risk are required to apply modifications to the calculation of the duration to reflect prepayment risk for debt instruments. The CRR investment firms shall apply one of the two methods for the correction to modified duration provided for in the EBA Guidelines on corrections to modified duration for debt instruments under the second subparagraph of Article 340(3) of Regulation (EU) 575/2013 (EBA/GL/2016/09).

Chapter 7. Risks associated with the custody of financial assets by third parties

36. The institutions shall have a policy for the selection of custodians which hold their customers' financial assets. This policy shall establish minimum quality criteria which a custodian must meet.
37. The institutions shall carry out due diligence controls before concluding an agreement with a custodian and they shall exercise an ongoing supervision of the custodian for the whole duration of the relationship in order to ensure that these quality criteria are met.
38. The institutions shall perform regular reconciliations between the assets recorded in their accounts as belonging to the customers and those confirmed by their custodians.

Commission de Surveillance du Secteur Financier

Part IV. Chronology and entry into force

- Circular CSSF 12/552 implementing the Guidelines of the European Banking Authority (EBA) on Internal Governance of 27 September 2011 ("GL44"), those of the Basel Committee on Banking Supervision (BCBS) on the internal audit function of 28 June 2012, the CEBS Guidelines published on 26 April 2010 (Principles for disclosures in times of stress (Lessons learnt from the financial crisis)), the CEBS Guidelines of 2 September 2010 on the management of concentration risk under the supervisory review process ("GL31") and the Guidelines of 27 October 2010 on Liquidity Cost Benefit Allocation.
- Circular CSSF 13/563 implementing the EBA Guidelines on the assessment of the suitability of members of the management body and key function holders dated 22 November 2012 (EBA/GL/2012/06) as well as the ESMA Guidelines on certain aspects of the MiFID compliance function requirements dated 6 July 2012 (ESMA/2012/388).
- Circular CSSF 14/597 implementing the Recommendation of the European Systemic Risk Board (ESRB) on funding of credit institutions (ESRB/2012/2), Recommendation B on the establishment of a general risk management framework for asset encumbrance.
- Circular CSSF 16/642 implementing the EBA Guidelines on the management of interest rate risk arising from non-trading activities (EBA/GL/2015/08).
- Circular CSSF 16/647 implementing the EBA Guidelines on limits on exposures to shadow banking entities which carry out banking activities outside a regulated framework under Article 395(2) of Regulation (EU) No 575/2013 (EBA/GL/2015/20).
- Circular CSSF 20/750 implementing the EBA Guidelines on ICT and security risk management (EBA/GL/2019/04).
- This Circular CSSF 20/758 repealing and replacing Circular CSSF 12/552, as amended by Circulars CSSF 13/563, CSSF 14/597, CSSF 16/642, CSSF 16/647, CSSF 17/655 and CSSF 20/750, for investment firms and which entered into force on 1 January 2021.
- Circular CSSF 21/785 replacing the prior authorisation obligation by a prior notification obligation in the case of material IT outsourcing.
- Circular CSSF 22/806 on outsourcing arrangements.

The guidelines and recommendations referred to in this Circular are available on the websites of the EBA (www.eba.europa.eu), ESMA, (www.esma.europa.eu) and the BCBS (https://www.bis.org/bcbs/index.htm).

The changes brought to Circular CSSF 20/758 come into force on 30 June 2022.

Commission de Surveillance du Secteur Financier

Claude WAMPACH
Director

Marco ZWICK
Director

Jean-Pierre FABER
Director

Françoise KAUTHEN
Director

Claude MARX
Director General

Annex: Extracts from Section 9.3 of EBA/GL/2017/12, independent members of a CRD-institution's management body in its supervisory function

Commission de Surveillance du Secteur Financier

Annex I - Extracts from Section 9.3 of EBA/GL/2017/12, independent members of a CRD-institution's management body in its supervisory function

91. Without prejudice to paragraph 92, in the following situations it is presumed that a member of a CRD-institution's management body in its supervisory function is regarded as not 'being independent':

a. the member has or has had a mandate as a member of the management body in its management function within an institution within the scope of prudential consolidation, unless he or she has not occupied such a position for the previous 5 years;

b. the member is a controlling shareholder of the CRD-institution, being determined by reference to the cases mentioned in Article 22(1) of Directive 2013/34/EU, or represents the interest of a controlling shareholder, including where the owner is a Member State or other public body;

c. the member has a material financial or business relationship with the CRD-institution;

d. the member is an employee of, or is otherwise associated with a controlling shareholder of the CRD-institution;

e. the member is employed by any entity within the scope of consolidation, except when both of the following conditions are met:

i. the member does not belong to the institution's highest hierarchical level, which is directly accountable to the management body;

ii. the member has been elected to the supervisory function in the context of a system of employees' representation and national law provides for adequate protection against abusive dismissal and other forms of unfair treatment;

f. the member has previously been employed in a position at the highest hierarchical level in the CRD-institution or another entity within its scope of prudential consolidation, being directly accountable only to the management body, and there has not been a period of at least 3 years, between ceasing such employment and serving on the management body;

g. the member has been, within a period of 3 years, a principal of a material professional adviser, an external auditor or a material consultant to the CRD-institution or another entity within the scope of prudential consolidation, or otherwise an employee materially associated with the service provided;

h. the member is or has been, within the last year, a material supplier or material customer of the CRD-institution or another entity within the scope of prudential consolidation or had another material business relationship, or is a senior officer of or is otherwise associated directly or indirectly with a material supplier, customer or commercial entity that has a material business relationship;

i. the member receives in addition to remuneration for his or her role and remuneration for employment in line with point (e) significant fees or other benefits from the CRD-institution or another entity within its scope of prudential consolidation;

j. the member served as member of the management body within the entity for 12 consecutive years or longer;

k. the member is a close family member of a member of the management body in the management function of the CRD-institution or another entity in the scope of prudential consolidation or a person in a situation referred to under points (a) to (h).

92. The mere fact of meeting one or more situations under paragraph 91 is not automatically qualifying a member as not being independent. Where a member falls under one or more of the situations set out in paragraph 91, the CRD-institution may demonstrate to the competent authority that the member should nevertheless be considered as 'being independent'. To this end CRD-institutions should be able to justify to the competent authority the reasoning why the members' ability to exercise objective and balanced judgement and to take decisions independently are not affected by the situation.

93. For the purposes of paragraph 92 CRD-institutions should consider that being a shareholder of a CRD-institution, having private accounts or loans or using other services, other than in the cases explicitly listed within this section, should not lead to a situation where the member is considered to be non-independent if they stay within an appropriate de minimis threshold. Such relationships should be taken into account within the management of conflicts of interest in accordance with the EBA Guidelines on Internal Governance.

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