cssf

Commission de Surveillance
du Secteur Financier

Circular CSSF 12/552

as amended by Circulars CSSF 13/563, CSSF 14/597, CSSF 16/642, CSSF 16/647, CSSF 17/655, CSSF 20/750 and CSSF 20/759

Central administration, internal governance and risk management

Commission de Surveillance du Secteur Financier

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

Circular CSSF 12/552

Re: Central administration, internal governance and risk management

Luxembourg, 7 December 2020

To all credit institutions and professionals performing lending operations[1]

Ladies and Gentlemen,

Articles 5(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") require credit institutions 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 credit institutions must take pursuant to the provisions of the LFS and RCSSF 15-02 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 banking 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 credit institutions shall refer to the principles set out in Chapter 2 of Part I and to the guidelines and recommendations listed in Part IV of this Circular 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).

The principles and good practices arising from other sources already included in the previous versions of the Circular have been maintained in so far as they have not become obsolete.

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

[1] *To professionals performing lending operations as defined in Article 28-4 of the Law of 5 April 1993 on the financial sector, Chapter 3 of Part III, with the exception of Sub-chapter 3.4 "Exposures associated with particularly high risk" shall apply. Chapter 2(12) of Part III shall also apply.*

Commission de Surveillance du Secteur Financier

The Circular is divided into four parts: the first part 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 and the history of the updates, allowing the reader to retrace the amendments entailed by the successive updates.

Commission de Surveillance du Secteur Financier

TABLE OF CONTENTS

1. Part I - Definitions and Scope

1.1 Chapter 1. Definitions and abbreviations

1. For the purposes of this Circular:

1) "competent authority" shall mean the European Central Bank ("ECB") for significant credit institutions ("significant institutions", "SI") or the Commission de Surveillance du Secteur Financier ("CSSF") for less significant credit institutions ("less significant institutions", "LSI")[2] and branches established in Luxembourg of third-country credit institutions.

Moreover, as host authority of Luxembourg branches of credit institutions authorised in another Member State, the CSSF retains the responsibility for the oversight of certain areas outside the banking prudential supervision, i.e. the fight against money laundering and terrorist financing, the rules applicable to the provision of investment services and the enforcement of the requirements applicable to Luxembourg UCI depositaries.

2) "authorised management" or "authorised managers" shall be deemed the management body in its management function in accordance with the EBA Guidelines on internal governance ("EBA/GL/2017/11"). The authorised managers shall be the persons referred to in Article 7(2) of the LFS and the senior management as defined in Article 3 of CRD IV.

From a prudential standpoint, the authorised management shall be in charge of the day-to-day management of an institution, in accordance with the strategic directions and the key policies approved by the supervisory body. In a one-tier system, the authorised managers may also be members of the Board of Directors, while in a two-tier system, the authorised management corresponds strictly to the Executive Board;

3) "institution" shall mean credit institutions incorporated under Luxembourg law, including their branches, Luxembourg branches of third-country credit institutions and Luxembourg branches of credit institutions authorised in another Member State;

[2] In accordance with Council Regulation (EU) No 1024/2013 of 15 October 2013 ("SSM Regulation") conferring specific tasks on the ECB concerning policies relating to the prudential supervision of credit institutions and with Regulation (EU) No 468/2014 of the European Central Bank establishing the framework for cooperation within the Single Supervisory Mechanism between the European Central Bank and national competent authorities and with national designated authorities ("SSM Framework Regulation").

4) "significant institution" shall mean systemically important credit institutions in accordance with Article 59-3 of the LFS and, if applicable, other credit institutions determined as such by the competent authority based on the assessment of the institutions' size and internal organisation as well as the nature, the scale and the complexity of their activities;

5) "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 the EBA Guidelines on internal governance ("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;

6) "supervisory body" shall correspond to the management body in its supervisory function in accordance with the EBA Guidelines on internal governance ("EBA/GL/2017/11") and to the members of the management body who do not perform any executive function within the meaning of the LFS. According to the financial sector regulation, boards of directors and supervisory boards of credit institutions are assigned responsibilities as regards the supervision and control, as well as the determination and approval of strategies and key principles;

7) "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 and members of the management body of these entities;

8) "Prudential Procedure" shall mean the prudential procedure for the appointment of members of the management body and key function holders in credit institutions;

9) "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;

10) CEBS shall mean the Committee of European Banking Supervisors;

11) CRD IV shall mean Directive 2013/36/EU of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC;

12) CRR shall mean Regulation (EU) No 575/2013 of 26 June 2013 on prudential requirements for credit institutions and investment firms;

13) EEA shall mean the European Economic Area;

14) ICAAP shall mean the Internal Capital Adequacy Assessment Process;

15) ILAAP shall mean the Internal Liquidity Adequacy Assessment Process;

16) LFS shall mean the Law of 5 April 1993 on the financial sector, as amended;

17) MiFID shall mean the Markets in Financial Instruments Directive.

1.2 Chapter 2. Scope and proportionality

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

   In respect of the areas for which the CSSF retains an oversight responsibility as host authority and as authority in charge of an area outside the banking prudential supervision, respectively - i.e. anti-money laundering and counter terrorist financing measures, rules applicable to the provision of investment services and requirements applicable to UCI depositaries – Luxembourg branches of credit institutions authorised in another Member State, in coordination with this institution, 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 Article 21a(1) of CRD IV and to credit institutions referred to in Article 21a(4)(c) of CRDI IV.

   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 supervisory body 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 audit. 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 shall 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 activities;
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 supervisory body.

2. Part II. Central administration and internal governance arrangements

2.1 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.

2.2 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 supervisory body, 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 supervisory body 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 management body sets ("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.

2.3 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 institutions 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").

2.4 Chapter 4. Supervisory body and authorised management

2.4.1 Sub-chapter 4.1. Supervisory body

2.4.1.1 Section 4.1.1. Responsibilities of the supervisory body

11. The supervisory body 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 supervisory body 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;
- the guiding principles governing the appointment and succession to the management body and to key functions in the institution, as well as the procedures governing the composition of the supervisory body, 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 accordance with the corporate governance, the guiding principles and procedures applicable to the members of the supervisory body are to be submitted, where applicable, to the shareholders for approval, under the Prudential Procedure as published on the CSSF website.*

12. The supervisory body 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 supervisory body and the procedures determining its operation).

13. The supervisory body 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 supervisory body 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 supervisory body 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 supervisory body 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 supervisory body 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) and the competent authority;

- the adequacy of the organisational and operational structure. The supervisory body 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 and ILAAP reports and the reports of the internal control functions which the supervisory body is called upon to approve on this occasion.

15. The supervisory body 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 supervisory body shall ensure that the work of these functions is performed in compliance with the recognised standards and under the approved policies.

16. The supervisory body shall ensure that sufficient time is devoted to risk issues.

17. Where the supervisory body 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 own funds or regulatory or internal liquidity reserves, it requires the authorised management to provide it with the corrective measures, without delay, and to inform the competent authority thereof forthwith. The obligation to notify the competent authority also concerns all information which casts doubt on the qualification or good repute of a member of the management body or the authorised management or a head of a key function.

2.4.1.2 Section 4.1.2. Composition and qualification of the supervisory body

18. The members of the supervisory body must be in sufficient number and, as a whole, must be composed adequately so that the supervisory body can fully meet its responsibilities. The adequacy of the composition of the supervisory body refers, in particular, to professional qualifications (adequate knowledge, skills and experience), as well as to the personal qualities of the members of the supervisory body. Moreover, each member must demonstrate his/her professional repute. The guiding principles governing the appointment and succession of the members of the supervisory body explain and provide for the abilities deemed necessary to ensure an appropriate composition and qualification of the supervisory body.

19. The supervisory body 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 supervisory body 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 supervisory body shall have a full understanding of the internal governance arrangements and of 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 supervisory body 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 supervisory body 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 supervisory body 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 supervisory body of the mandates they have outside the institution.

21. The terms of reference of the mandates must be laid down so that the supervisory body 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 supervisory body must be ensured.

22. The guiding principles governing the appointment and succession of the members of the supervisory body 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 supervisory body, 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. Each institution should appoint at least one member to its supervisory body who may be considered as "independent member".

    An independent member of the supervisory body 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 supervisory body has a sufficient number of independent members, considering their organisation and the nature, the scale and the complexity of their activities.

2.4.1.3 Section 4.1.3. Organisation and functioning of the supervisory body

24. The supervisory body shall regularly meet in order to effectively fulfil its responsibilities. The organisation and functioning of the supervisory body 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 supervisory body 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 supervisory body. The minutes are an important tool which must, on the one hand, help the supervisory body and its members monitor the decisions and, on the other hand, enable the body and its members to be accountable to the shareholders and the competent authorities. Thus, the routine items may be included in the minutes of a meeting succinctly, 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 supervisory body 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 supervisory body and specialised committees that depend on it.

27. The chairperson of the supervisory body 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 supervisory body and to propose the appointment of independent members. The chairperson of the supervisory body shall not exercise executive functions within the institution, save in exceptional situations to be authorised by the competent authority.

2.4.1.4 Section 4.1.4. Specialised committees

28. The supervisory body 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. Their missions shall be to provide the supervisory body 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 experience 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 supervisory body 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 supervisory body 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 supervisory body. 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 supervisory body 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 supervisory body 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 supervisory body on a regular basis.

37. The supervisory body cannot delegate its powers and responsibilities pursuant to this Circular to the specialised committees. Where it 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 it.

2.4.1.4.1 Sub-section 4.1.4.1. Audit committee

38. The purpose of the audit committee shall be to assist the supervisory body 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 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.

42. The audit committee shall regularly and critically deliberate on the following[4]:

- 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;

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

- 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 supervisory body 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 supervisory body 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.

2.4.1.4.2 Sub-section 4.1.4.2. Risk committee

44. The purpose of the risk committee shall be to advise the supervisory body 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.

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 supervisory body 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 supervisory body in the recruitment of external experts that the supervisory body 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 supervisory body 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 supervisory body or of any other specialised committee.

2.4.2 Sub-chapter 4.2. Authorised management

2.4.2.1 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 supervisory body 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 supervisory body and the competent authorities. 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 7(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 shall perform its duties as a permanent function within the institution; it must be on site.

54. The authorised management shall implement, through written internal policies and procedures, all the strategies and guiding principles laid down by the supervisory body 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 supervisory body, 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 and the members of the management body 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 supervisory body 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 supervisory body which must authorise time extensions for the implementation of these measures.

The institution shall establish a similar procedure, approved by the supervisory body, which shall apply where the competent authority 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 supervisory body and the competent authority.

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 supervisory body, 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 competent authority 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.

    The information to be provided pursuant to the first paragraph must be submitted together with the annual accounts to be published to the competent authority.

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 supervisory body and the competent authority 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 competent authority. Thus, s/he shall ensure that the form and content of this information comply with the legal rules and instructions of the competent authority 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 competent authority 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.

2.4.2.2 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 (knowledge, skills and experience), the good 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.

2.5 Chapter 5. Administrative, accounting and IT organisation

2.5.1 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 supervisory body.

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 7(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. Moreover, if in an institution limited in size and activity, and composed of only two authorised managers, there are conflicts of interest between these two managers following the assignment of the risk-taking function and the risk control function and if these conflicts of interest cannot be mitigated effectively, a third authorised manager shall be appointed.

72. The institution shall have a continuing vocational training programme which shall ensure that the staff members as well as the management body 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.

2.5.2 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); and
    - 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.

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

77. The files, working papers and control reports of the internal control functions, experts and subcontractors referred to in Sub-chapter 6.2 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 competent authority 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.

2.5.3 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.

2.5.3.1 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.

2.5.3.2 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 competent authority.

    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 supervisory body.

82. 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 competent authority;
    - the production and transmission of periodic information, including, primarily, the legal and regulatory reporting, to the competent authority, 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.

83. 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.

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

85. 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.

86. 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.

87. 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.

88. 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.

2.5.3.3 Section 5.3.3. IT function

89. 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.

90. The institutions, which rely on third parties as regards the IT function, shall comply, in particular, with the conditions laid down in Sub-chapter 7.4 of this part.

2.5.3.4 Section 5.3.4. Communication and internal and external alert arrangements

91. 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 management body, 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.

92. 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 management body and staff of the institution, considering their information needs, their responsibilities within the institution and the objective to ensure a sound and prudent business management.

93. 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 supervisory body. The alerts issued in good faith shall not result in any liability or adverse impact of any sort for the persons who issued them.

94. 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).

2.5.3.5 Section 5.3.5. Crisis management arrangements

95. 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.

96. The crisis management arrangements shall ensure that, in times of stress, the credit institutions provide the public with the information referred to in the CEBS guidelines published on 26 April 2010 ("Principles for disclosures in times of stress (Lessons learnt from the financial crisis)").

97. The crisis management arrangements shall include 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.

2.6 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 competent authority are met[5].

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.

[5] *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, safekeeping of securities of third parties (depositary bank), bookkeeping and net asset value calculation of investment funds.*

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.

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.

2.6.1 Sub-chapter 6.1. Operational controls

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

2.6.1.1 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.

2.6.1.2 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 (in particular as regards credits);
- 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 (in particular as regards market and credit activities);
- 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.

2.6.1.3 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 these persons 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, non-performing loan exposures, restructured credits 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 their colleagues of the authorised management about the exercise of their control function, on a regular basis.

2.6.2 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.

2.6.2.1 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 supervisory body and, where appropriate, to the specialised committees. They shall provide the authorised management and the supervisory body, 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 supervisory body 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 supervisory body of the group head.

2.6.2.2 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 supervisory body or its chairperson or, where appropriate, to the specialised committees which are part of it, to the *réviseur d'entreprises agréé* of the institution as well as to the competent authority.

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 banking and 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.

2.6.2.3 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 supervisory body 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 supervisory body or the competent specialised committees to ensure its follow-up and that the supervisory body 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 supervisory body 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. 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 supervisory body and reported in writing to the competent authority 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 supervisory body 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 supervisory body 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.

119. Outsourcing of the compliance function and risk control function is not authorised.

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 supervisory body 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 have direct access to the supervisory body or, where appropriate, the chairperson of the audit committee.

120. 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 supervisory body 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 supervisory body shall approve the external resources selected by the authorised management.

121. 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.

122. 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 a compliance function or for appointing two heads of these functions full time, the institution may set up a combined function or a position with combined responsibility, subject to prior approval of the competent authority.

However, the application of the principle of proportionality may not result in the accumulation of other responsibilities for a person already combining the responsibility for the risk control function and the compliance function.

The institution wishing to create a combined risk control and compliance function, allocate the responsibilities for these two functions to one single person or combine one of these responsibilities with other tasks must submit a request to the competent authority which shall include:

- a description of the combined function or the position with combined responsibility;
- the analysis of its conclusions justifying the creation of a combined function or a position with combined responsibility given the institution's organisation, the nature, scale and complexity of its activities and risks; and
- the decision of the supervisory body approving the analysis and its conclusions.

123. The institution wishing, in accordance with the principle of proportionality, to outsource the operational tasks of the internal audit function must submit a prior request to the competent authority which shall include:
    - the description of the outsourcing, the provider chosen, the contracted external resources and the name of the head of the external team fulfilling the internal audit duties; as well as
    - the person in charge of this outsourcing within the institution;
    - the analysis and its conclusions justifying the outsourcing of the operational tasks of the internal audit function; and
    - the decision of the supervisory body approving the analysis and its conclusions and, where appropriate, the opinion of the audit committee.

    These external providers may be the internal auditors of the group to which the institution belongs. The supervisory body 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.

124. 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.

125. 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 heads of the control functions in the group head must give their consent for any recruitment, dismissal and significant decisions regarding the remuneration of the heads of the control functions in branches and/or subsidiaries. The reports drawn up in accordance with the provisions of this Circular shall be submitted not only to the local management and supervisory body but also, in summarised form, to the internal control functions of the group head which shall analyse them and report the points to be noted in accordance with point 116.

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 116.

126. 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

127. 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 supervisory body 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 supervisory body. Thus, the term "risk control function" shall not reduce this function to a simple ex-post "control" of the limits.

128. 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.

129. 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.

130. The head of the risk control function shall ensure that the authorised management and the supervisory body receive an independent, comprehensive, objective and relevant overview of the risks to which the institution is or may be exposed[6]. 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 supervisory body. 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 competent authority, 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.

131. 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.

132. 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 supervisory body 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).

133. 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.

[6] *In line with "Principles for effective risk data aggregation and risk reporting" (BCBS 239) of January 2013.*

Sub-section 6.2.5.2. Organisation of the risk control function

134. 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.

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 supervisory body.

    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 Guidelines 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 supervisory body.

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 are used;
- establish the right for the Chief Compliance Officer to, directly and on his/her own initiative, contact the chairperson of the supervisory body or, where appropriate, the members of the audit committee or the compliance committee as well as the competent authority.

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 supervisory body. 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 competent authority, 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 supervisory body) or external (for instance reports of the *réviseur d'entreprises agréé*, correspondence from the supervisory authority).

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

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.

Section 6.2.7. Internal audit function

Sub-section 6.2.7.1. Internal audit charter

147. 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 ultimately approved by the supervisory body.

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 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 contact, directly and on his/her own initiative, the chairperson of the supervisory body or, where appropriate, the members of the audit committee as well as the competent authority;
- specify the recognised professional standards governing the functioning and work of the internal audit[7];
- specify the procedures to be observed in respect of coordination and cooperation with the *réviseur d'entreprises agréé.*

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 amendments must be ultimately approved by the supervisory body. They shall be brought to the attention of all staff members.

148. 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.

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

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

149. The internal audit function shall examine and assess, among others (non-exhaustive list[8]), 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 competent authority;
- effectiveness and efficiency of central administration, governance and internal control arrangements, including the risk control and compliance functions;
- safeguarding of the values and assets;
- 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 supervisory body and, where appropriate, the specialised committees, to the authorised management and the competent authority;
- compliance with the policies and procedures, in particular those governing capital adequacy and internal liquidity reserves;
- 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.

[8] *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.*

150. 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.

151. 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

152. 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 supervisory body or, where appropriate, the audit committee as well as the authorised management. The plan shall cover all matters of prudential interest (including the competent authority's observations and requests) and shall also reflect the developments and innovations provided for as well as the risks which may arise therefrom.

153. The plan shall be discussed with the authorised management and, where appropriate, with the audit committee and ultimately approved by the supervisory body. 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 supervisory body. 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 supervisory body, the internal audit shall indicate and state the reasons for the main changes brought to the audit plan as initially approved by the supervisory body: cancelled missions, delayed missions as well as the missions whose scope has significantly changed.

154. 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.

155. 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.

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

157. 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.

158. Each mission shall be the subject of a written report of the internal audit department, in general, intended for the audited persons, the authorised management as well as - possibly in summarised form - for the supervisory body (and, where appropriate, the audit committee). The reports shall also be made available to the *réviseur d'entreprises agréé* and the competent authority. 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

159. 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.

160. In case the operational tasks of the internal audit are outsourced, the external 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 authorised management, where appropriate, the audit committee and the supervisory body.

Chapter 7. Specific requirements

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

161. 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.

162. The guiding principles that the supervisory body 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 supervisory body, the authorised management, the internal control functions or the competent authority upon their request.

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

163. 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 banking standards.

164. The guiding principles regarding internal governance, which the supervisory body 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

165. 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 third-party subcontractors. This policy shall be applicable to all staff as well as to the authorised management and members of the supervisory body.

166. 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.

167. 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.

168. 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.

169. The policy in question 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 supervisory body, who are subject to a conflict of interest, shall promptly inform the authorised management or the supervisory board, 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.[9]

170. 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

171. The transactions with related parties shall be subject to the supervisory body's 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.

172. Any material change in significant transactions carried out with related parties must be brought to the attention of the supervisory body as soon as possible.

173. 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.

174. 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.

[9] *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.*

Sub-chapter 7.3. New Product Approval Process

175. 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 supervisory body, the risk strategy, the risk appetite of the institution and the corresponding limits.

176. 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.

177. 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.

178. 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.

179. 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

180. Outsourcing shall mean the complete or partial transfer of the operational tasks, activities or services of the institution to an external service provider, whether or not it is part of the group to which the institution belongs.

For the purposes of this sub-chapter, the term “activity” shall refer to the operational tasks, activities and services mentioned in the first paragraph. Any activity that, when it is not carried out in accordance with the rules, reduces the institution's ability to meet the regulatory requirements or to continue its operations as well as any activity necessary for the sound and prudent risk management shall be deemed to be “material”.

181. Where outsourcing or an outsourcing chain concerns purely services that are IT in nature and where at least one outsourcing meets the definition of cloud computing under Circular CSSF 17/654, the requirements of this sub-chapter shall not apply and the institution shall comply with the requirements of Circular CSSF 17/654.

The exception laid down in the preceding paragraph shall not apply to business process outsourcing relying on an outsourced cloud computing infrastructure.

Section 7.4.1. General outsourcing requirements

182. Outsourcing must not result in non-compliance with the rules of this Circular on central administration.

The outsourcing institution shall, in particular, comply with the following requirements:

- The strategic functions or core functions cannot be outsourced;
- The institution shall retain the necessary expertise to effectively monitor the outsourced services or tasks and the management of the risks associated with the outsourcing;
- The institution shall ensure protection of the data concerned by an outsourcing in accordance with the General Data Protection Regulation (GDPR) and with the requirements of the authority competent in this matter, the National Commission for Data Protection (CNPD);
- In case of outsourcing, the institution shall apply the provisions of Article 41(2a) of the LFS with respect to professional secrecy;
- The outsourcing does not relieve the institution of its legal and regulatory obligations or its responsibilities to its customers. It shall not result in the delegation of the institution’s responsibility to the subcontractor;
- The final responsibility for the management of risks associated with outsourcing shall lie with the institution which is outsourcing;
- The confidentiality and integrity of data and systems must be controlled throughout the outsourcing chain. In particular, access to data and systems must fulfil the principles of “need to know” and “least privilege”, i.e. access shall only be granted to persons whose functions so require, for a specific purpose, and their privileges shall be limited to the strict necessary minimum to exercise their functions;

- The institution which intends to outsource a material activity must obtain prior authorisation from the competent authority. A notification to the competent authority justifying that the conditions laid down in this Circular are complied with is sufficient where the institution resorts to a Luxembourg credit institution or a support PFS in accordance with Articles 29-1 to 29-6 of the LFS;
- The access of the competent authority, the *réviseur d'entreprises agréé* and the internal control functions of the institution to the information relating to the outsourced activities must be guaranteed in order to enable them to issue a well-founded opinion on the adequacy of the outsourcing. This access implies that they may also verify the relevant data held by an external partner and, in the cases provided for in the applicable national law, have the power to perform on-site inspections of an external partner. The aforementioned opinion may be, where appropriate, based on the reports of the subcontractor's external *réviseur* (auditor).

183. The outsourcing institution shall base its decision to outsource on a prior and in-depth analysis demonstrating that it does not result in the relocation of the central administration. This analysis shall include at least a detailed description of the services or activities to be outsourced, the expected results of the outsourcing and an in-depth assessment of the risks of the contemplated outsourcing project as regards financial, operational, legal and reputational risks. The analysis shall include a detailed (due diligence) assessment of the proposed service provider.

184. Special attention must be paid to the outsourcing of critical activities in respect of which the occurrence of a problem may have a significant impact on the institution's ability to meet the regulatory requirements or even to continue its activities.

185. Special attention must be paid to the concentration and dependence risks which may arise when large parts of activities or important functions are outsourced to a single provider during a sustained period.

186. The institutions must take into account the risks associated with the outsourcing "chains" (where a service provider outsources part of the outsourced activities to other service providers). In this respect, they shall take particular account of the safeguarding of the integrity of the internal and external control. Moreover, the institution shall ensure to provide the competent authority with any elements proving that the sub-outsourcing process is under control.

187. The outsourcing policy shall take into account the impact of the outsourcing on the institution's activities and risks, in particular, the operational risks arising therefrom, such as legal risk, IT risk, reputational risk or concentration risk (at the level of service providers). It shall lay down the applicable requirements regarding outsourcing to which the service providers are subject, from the preparation phase to the expiry or termination and through the reporting, and determine the control mechanism which the institution implements in this respect from inception to the end of the outsourcing agreement. Outsourcing may, in no circumstances, lead to the circumvention of any regulatory restrictions or prudential measures of the competent authority or the challenge of its supervision.

188. Special attention must be paid to the continuity aspects and the revocable nature of outsourcing. The institution must be able to continue its critical functions in case of exceptional events or crisis. In this respect, the outsourcing agreements shall provide for a notice of termination which shall give sufficient time to the institution to take the necessary measures to ensure continuity of the outsourced services and shall not include any termination clause or service termination clause because of resolution actions or reorganisation measures or a winding-up procedure applied to the institution, as laid down in the Law of 18 December 2015 on the failure of credit institutions and certain investment firms. The institution shall also take the necessary measures to be in a position to adequately transfer the outsourced services to a different provider or to bring them in-house whenever the continuity or quality of the service provision is likely to be affected.

189. For each outsourced activity, the institution shall designate, from among its staff, a person who will be in charge of managing the outsourcing relationship and managing access to confidential data.

Section 7.4.2. Specific IT outsourcing requirements

190. The institution shall implement an IT policy which covers all IT activities distributed among the institution and all the actors in the outsourcing chain. The IT organisation shall be adapted in order to integrate the outsourced activities to the proper functioning of the institution and the procedures manual shall be adapted accordingly. The institution's continuity plan shall be established in accordance with the continuity plan of its subcontractor(s). The institution shall also provide for the regular testing of backups and of the facilities to restore backups.

191. The institution's policy on information systems security shall consider the individual security implemented by its subcontractor(s), in order to ensure overall consistency.

192. IT outsourcing may cover consulting, development and maintenance services (Sub-section 7.4.2.2), hosting services (Sub-section 7.4.2.3) or IT system management/operation services (Sub-section 7.4.2.1).

Sub-section 7.4.2.1. IT system management/operation services

193. The institutions may contractually use services for the management/operation of their systems:

- In Luxembourg, solely from:
  - a credit institution or a financial professional holding a support PFS authorisation in accordance with Articles 29-3 and 29-4 of the LFS (primary IT systems operators of the financial sector or secondary IT systems and communication networks operators of the financial sector);
  - an entity of the group to which the institution belongs, which exclusively processes group transactions. In case these systems include readable confidential data of customers, the institution shall ensure compliance with the provisions of Article 41(2a) of the LFS.
- Abroad, from:
  - any IT service provider, including from an entity of the group to which the institution belongs. In case these systems include readable confidential data of customers, the institution shall ensure compliance with the provisions of Article 41(2a) of the LFS.

Sub-section 7.4.2.2. Consulting, development and maintenance services

194. The consulting, development and maintenance services may be contracted with any IT service provider, including an IT service of the group to which the institution belongs or a support PFS.

195. Third-party subcontractors which provide consulting, development or maintenance services must operate by default outside the IT production system. Formal agreement of the institution is required for each intervention on the production system. If an exceptional situation requires an intervention on the production system and if the access to confidential data cannot be avoided, the institution must ensure that the third party in question is supervised throughout its mission by a person of the institution in charge of IT and that the provisions of Article 41(2a) of the LFS are complied with.

196. Any change in the application functionality by a third party - other than changes relating to corrective maintenance - must be submitted for approval to the institution prior to its implementation.

197. The institution shall ensure that there are, if needed, no legal obstacles to obtain access to the operating systems which have been developed by this third-party subcontractor. This can be achieved, for example, when the institution is the legal owner of the programmes. The institution shall ensure that it is possible to continue operating the applications which are critical for the activity in the event of a subcontractor's failure, for a period compatible with a transfer of this outsourcing to another subcontractor or a takeover of the applications concerned by the institution itself.

Sub-section 7.4.2.3. Hosting services and infrastructure ownership

198. The IT infrastructure may be owned by the institution or be provided by the subcontractor.

Where the IT infrastructure includes readable confidential data of customers, the institution shall ensure compliance with the provisions of Article 41(2a) of the LFS. Otherwise, the subcontractor cannot operate on the infrastructure of the institution without being accompanied, throughout its mission, by a person of the institution in charge of IT.

Formal agreement of the institution is required for each intervention on the IT infrastructure by a third party, except for interventions carried out by a support PFS as part of its mandate as operator.

199. It is not mandatory for the processing centre to be physically located in the premises of the entity which is contractually responsible for the management of the IT systems. Whether the processing centre is in Luxembourg or abroad, it is thus possible that the hosting of the site is entrusted with another provider than the one providing IT system management services. In this case, the institution must ensure that the principles set out in this sub-chapter are complied with by the entity which is contractually responsible for the management of IT systems and that the sub-outsourcing process is under control.

200. Where the processing centre is in Luxembourg, it may be hosted at a provider other than a credit institution or a support PFS, provided that it does not act as operator. If the provider has physical or logical access to the institution's systems, the institution shall ensure compliance with the provisions of Article 41(2a) of the LFS.

201. Where the processing centre is abroad, no confidential data which enables the identification of a customer of the institution can be stored therein unless it is protected. The confidentiality and integrity of data and systems must be controlled throughout the outsourcing chain. In particular, access to data and systems must fulfil the principles of "need to know" and "least privilege", i.e. access shall only be granted to persons whose functions so require, for a specific purpose, and their privileges shall be limited to the strict necessary minimum to perform their functions. The institution shall ensure compliance with the provisions of Article 41(2a) of the LFS.

Section 7.4.3. Additional general requirements

202. In order to enable the institution to assess the reliability and completeness of the data produced by the IT system as well as its compatibility with the accounting and internal control requirements, one person, among its staff members, must have the necessary IT knowledge to understand both the impact of the programmes on the accounting system and the actions performed by the third party within the context of the provided services.

    The institution must also have, in its premises, sufficient documentation on the programmes used.

203. In case of IT service provision via telecommunication, the institution must ensure that:

    - sufficient safeguards are taken in order to avoid that non-authorised persons access its system. The institution must, in particular, make sure that telecommunications are encrypted or protected through other available technical resources so as to ensure the security of communication;
    - the network link enables the Luxembourg institution to have quick and unlimited access to the information stored in the processing unit (i.e. through an appropriate access path and data rate and through redundancy).

204. The institution must ensure that the capture, printing, backup, storage and archiving mechanisms guarantee the confidentiality of the data.

205. Outsourcing must not result in the transfer of the financial and accounting function to a third party. The institution shall have, at the closing of each day, the balance of all accounts and of all accounting movements of the day. The system must allow keeping regular accounts in accordance with the standards applicable in Luxembourg and thus respecting the form and content rules imposed by the Luxembourg accounting laws and regulations.

Section 7.4.4. Documentation

206. Any outsourcing of material or non-material activities, including that carried out within the group to which the institution belongs, shall be in line with a written policy requiring approval from the authorised management and including the contingency plans and exit strategies. This outsourcing policy shall be updated and re-approved, at regular intervals, by the supervisory body so that appropriate changes are rapidly implemented by the authorised management. Any outsourcing approval shall be the subject of an official and detailed contract (including specifications).

207. The written documentation shall also provide a clear description of the responsibilities of the two parties as well as the clear communication means accompanied by an obligation for the external service provider to report any significant problem having an impact on the outsourced activities as well as any emergency situation.

208. The institutions shall take the necessary measures to ensure that the internal control functions have access to any documentation relating to the outsourced activities, at any time and without difficulty, and that these functions retain the full opportunity to exercise their controls.

Chapter 8. Legal reporting

209. The credit institutions shall provide the competent authority with the ICAAP/ILAAP reports and the annual certificate of compliance with the requirements of this Circular as well as the summary reports of the internal control functions in accordance with the requirements of Circular CSSF 15/602. 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 institution is 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 supervisory body 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, the risk policy shall take due account of concentration risks.

4. The capital and liquidity policy implementing the strategy of the supervisory body 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 supervisory body 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.

12. For institutions operating on the domestic market, there is generally a concentrated exposure to the Luxembourg real estate market. A significant market downturn would undermine the financial stability of these institutions and have an adverse impact on the image of the Luxembourg financial centre as a whole. Consequently, the institutions shall implement prudent policies as regards the granting of real estate mortgage credits pursuant to Sub-chapters 3.2 and 3.3.

Chapter 3. Credit risk

Sub-chapter 3.1. General principles[10]

13. Risk-taking within the meaning of this sub-chapter shall mean not only the decisions on new credits to be granted, but also the decisions made in the context of the restructuring or renegotiation of exiting credits, particularly following a significant deterioration of the debtor's creditworthiness. The restructuring and renegotiations (forbearance) shall comprise, in particular, granting extensions, deferrals, renewals or amendments of the credit terms, including the repayment plan and any forbearance measures within the meaning of Article 49b of the CRR and non-performing loans within the meaning of Article 47a(3) of the CRR.

14. Each credit risk-taking must be subject to a written analysis which shall cover at least the debtor's creditworthiness, the repayment plan and the borrower's repayment ability over the period of the borrowing. In particular, the credit decision cannot be based on an exclusive analysis of collateral or other credit risk mitigation techniques. The institutions shall take into account the overall debt level of the debtor or the group of associated debtors, respectively.

    Regular repayments cannot exceed an amount which would not allow the borrower to have an adequate disposable income. There must be a reasonable security margin in order to cover an increase in interest rates.

15. Each credit risk-taking must be subject to a predetermined decision-making process which shall also involve a body separate from the business function.

    For low credit risk-taking, the institutions may put in place a grant-making process which enables them to monitor this risk-taking, as a whole, without necessarily going through the decision-making processes and individual analyses as referred here.

[10] *Supplementing the provisions of Article 9 of RCSSF 15-02 regarding credit and counterparty risk.*

The institutions shall be in charge of internally defining the concept of "low" credit risk for the purposes of the preceding paragraph. This definition shall focus at least on the institution's ability to manage, bear and control these risks, on the one hand, and on the exposure amount and credit quality of the debtor and transaction, on the other hand.

Sub-chapter 3.2. Residential real estate mortgage credit to individuals

16. The institutions shall apply a prudent credit granting policy which aims to safeguard their financial stability regardless of the observed or expected developments in the residential real estate market. This policy shall focus on healthy values of debt ratios and ratios between debt burden and income for the whole credit duration, as well as between the amount of the credit granted and the value of the obtained guarantees (loan-to-value), including the underlying mortgage on the property, based on prudent assessment methods.

Sub-chapter 3.3. Credits to real estate developers

17. Each real estate development project financing must provide for a start date of the principal repayment when the credit is granted. This date cannot exceed a reasonable time limit as regards the beginning of the project financing. When this time limit is exceeded, the file shall be automatically classified under the list of credits "in default" within the meaning of Article 178 of the CRR, Article 14 of CSSF Regulation 18-03 and EBA/GL/2016/07 and the full provisioning of unpaid interest.

    The real estate development financing must not only be based on the developer's reputation. In particular, it must take into consideration all the other factors which enable the assessment of the developer's strength, the legal structuring and the financial strength of the project, the environment in which the projects are carried out, their development phases and all the related guarantees and insurance.

    Moreover, the financing must be covered, in addition to the mortgage on the financed object, by a personal guarantee of the developer unless other guarantees or securities significantly cover the total cost of the financed object.

    The institutions shall set an internal limit for aggregate exposure they incur on the real estate development sector. Without prejudice to the rules applicable regarding large exposures (Part Four of the CRR), the completion bank guarantees may be excluded from this aggregate limit as far as the completion costs are adequately covered by pre-sale or pre-lease rates. This limit must be in healthy proportion to their regulatory capital.

It should be borne in mind that speculative immovable property financing as defined in Article 4(1)(79) of the CRR are deemed exposures associated with particularly high risk. In this respect, they shall be assigned a risk weight of 150%, as defined in Article 128(2)(d) of the CRR, under the standardised approach for credit risk.

Sub-chapter 3.4. Exposures associated with particularly high risk

18. The institutions applying a standardised approach for credit risk shall put in place a process to identify exposures associated with particularly high risk. This process shall cover at least the exposures within the meaning of Article 128(2) and (3) of the CRR.

19. The institutions shall apply Guidelines EBA/GL/2019/01 which specify the terms "investment in venture capital firms" and "investment in private equity" as defined in Article 128(2)(a) and (c) of the CRR. These Guidelines also specify which types of exposures, other than those mentioned in Article 128(2) of the CRR, must be associated with particularly high risk and under which circumstances.

    The types of exposures identified by the institutions as carrying a particularly high risk of loss, without however meeting the specific characteristics described in EBA/GL/2019/01, must be notified to the competent authority by using the corresponding form available on the CSSF website.

Sub-chapter 3.5. Non-performing and forborne exposures

20. The institutions shall have sound arrangements for the identification and management of commitments whose contractual maturity dates set for the payment of principal and/or interests have expired.

    To this end, the institutions shall have policies in place which define the measures to be taken where a debtor does not comply with or indicates to the bank that s/he is no longer able to comply with the contractual provisions of his/her commitment, in particular the various payment deadlines.

    In addition, the institutions shall have sound arrangements for the identification, management and provisioning of commitments "in default" within the meaning of Article 178 of the CRR, Article 14 of CSSF Regulation No 18-03 and EBA/GL/2016/07.

21. The institutions must maintain a list of commitments on a debtor or group of related debtors, whether they are forborne within the meaning of Article 49b of the CRR, non-performing within the meaning of Article 47a(3) of the CRR or "in default". These commitments shall be subject to periodic and objective review which must enable the institution to acknowledge and carry out the impairment and provisions of assets as required.

22. The institutions must have appropriate practices regarding governance and risk management of their non-performing exposures[11], their forborne exposures[12] and foreclosed assets in order to efficiently and sustainably reduce non-performing exposures in their balance sheets in accordance with the requirements of Circular CSSF 20/751.

Chapter 4. Risk transfer pricing

23. 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.

24. 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.

25. 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 5. Private wealth management ("private banking")

26. Private banking activity is especially exposed to money laundering and terrorist financing risks. Consequently, the institutions 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.

27. The 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.

[11] *Exposures classified as non-performing in accordance with Annex V of Commission Implementing Regulation (EU) No 680/2014.*

[12] *Exposures for which forbearance measures were applied in accordance with Annex V of Commission Implementing Regulation (EU) No 680/2014.*

28. The 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.

29. The 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.

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

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

32. 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.

33. The institutions must have sound arrangements in respect of credit control and bank overdraft within the context of the private banking activities. 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. The 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 6. Exposures to shadow banking entities

Sub-chapter 6.1. Implementation of sound internal control principles

34. The 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[13] in accordance with EBA/GL/2015/20.

35. The 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%[14] of the institution's eligible capital[15], after taking into account the effect of the credit risk mitigation and exemptions[16], must be taken into consideration and cannot be deemed as low exposure.

36. The 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 6.2. Application of quantitative limits

37. The 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.

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

39. When setting an aggregate limit to exposures to shadow banking entities, each institution must take into account:

- its business model, risk management framework and risk appetite;

[13] 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".

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

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

[16] 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.

- 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.

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

41. When setting those limits, as part of their internal assessment process, the 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.

42. If 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”).

43. 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 6.1, but cannot gather sufficient information to enable them to set out appropriate limits as set out in Sub-chapter 6.2, 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 6.2 must be applied to the remaining exposures to shadow banking entities.

Chapter 7. Asset encumbrance

44. The institutions shall put in place risk management policies to define their approach to asset encumbrance as well as procedures and controls that ensure that the risks associated with collateral management and asset encumbrance are adequately identified, monitored and managed. These policies shall take into account each institution's business model, the Member States in which they operate, the specificities of the funding markets and the macroeconomic situation. The policies must be approved by the supervisory body.

45. The institutions shall have in place a general monitoring framework that provides timely information, at least once a year, to the authorised management and the supervisory body on:

- the level, evolution and types of asset encumbrance and related sources of encumbrance, such as secured funding or other transactions;
- the amount, evolution and credit quality of unencumbered but encumberable assets, specifying the volume of assets available for encumbrance;
- the amount, evolution and types of encumbrance on additional assets resulting from stress scenarios (contingent encumbrance).

46. The institutions shall include, in their business continuity plan, actions to address the contingent encumbrance resulting from relevant stress events, which means plausible albeit unlikely shocks, including downgrades in the credit institution's credit rating, devaluation of pledged assets and increases in margin requirements.

Chapter 8. Interest rate risk

Sub-chapter 8.1 Interest rate risk arising from non-trading book activities

47. When implementing Article 14 (Interest rate risk arising from non-trading book activities) of RCSSF 15-02, the institutions shall comply with EBA/GL/2018/02.

Commission de Surveillance du Secteur Financier

Sub-chapter 8.2. Corrections to modified duration for debt instruments

48. The institutions 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 institutions shall apply one of the two methods for the correction to modified duration provided for in EBA/GL/2016/09.

Chapter 9. Risks associated with the custody of financial assets by third parties

49. The institutions shall have a policy for the selection of sub-custodians which hold their customers' financial assets. This policy shall establish minimum quality criteria which a sub-custodian must meet.

50. The institutions shall carry out due diligence controls before concluding an agreement with a sub-custodian and they shall exercise an ongoing supervision of the sub-custodian for the whole duration of the relationship in order to ensure that these quality criteria are met.

51. The institutions shall perform regular reconciliations between the assets recorded in their accounts as belonging to the customers and those confirmed by their sub-custodians.

Part IV. Chronology

- 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 in banks 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 12/522 cancels and replaces Circulars IML 93/94 and CSSF 10/466, as well as Circulars IML 95/120, IML 96/126, IML 98/143, CSSF 04/155 and CSSF 05/178 for credit institutions.

- 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).
- Circular CSSF 20/759 implementing the EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2017/11), the Joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body and key function holders (EBA/GL/2017/12), the EBA Guidelines on the application of the definition of default under Article 178 of Regulation (EU) No 575/2013 (EBA/GL/2016/07), the EBA Guidelines on specification of types of exposures to be associated with high risk (EBA/GL/2019/01), the EBA Guidelines on the management of interest rate risk arising from non-trading book activities (EBA/GL/2018/02) and 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).

  The above-mentioned guidelines and recommendations are available on the websites of the EBA (www.eba.europa.eu), ESMA, (www.esma.europa.eu), the BCBS (https://www.bis.org/bcbs/index.htm) and the ESRB (www.esrb.europa.eu).

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