Commission de Surveillance
du Secteur Financier

Circular CSSF 20/757

Introduction of Circular CSSF 20/758 on central administration, internal governance and risk management, and repeal of Circular CSSF 12/552 for investment firms (as amended by Circulars CSSF 13/563, 14/597, 16/642, 16/647, 17/655 et 20/750) on central administration, internal governance and risk management

Commission de Surveillance du Secteur Financier

We inform you that point 182 (8th indent) of the Annex to Circular CSSF 20/759 as well as point 184 (8th indent) of Annex 1 to Circular CSSF 20/757 have been updated on 11 December 2020.

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

Circular CSSF 20/757

Re: Introduction of Circular CSSF 20/758 on central administration, internal governance and risk management, and repeal of Circular CSSF 12/552 for investment firms (as amended by Circulars CSSF 13/563, 14/597, 16/642, 16/647, 17/655 et 20/750) on central administration, internal governance and risk management

Luxembourg, 7 December 2020

To all investment firms

Ladies and Gentlemen,

1. By way of this Circular, the CSSF, in its capacity as competent authority, complies with the guidelines of the European Banking Authority (EBA) and the joint guidelines of the EBA and the European Securities and Markets Authority (ESMA) listed in point 2. The CSSF has integrated these guidelines into its administrative practice and regulatory approach with a view to promote supervisory convergence in this field at European level.

2. The following guidelines are concerned:

(a) Guidelines on internal governance (EBA/GL/2017/11);

(b) 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);

(c) Guidelines on the management of interest rate risk arising from non-trading book activities (EBA/GL/2018/02)[1];

(d) 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)[2].

3. This Circular repeals Circular CSSF 12/552 on the central administration, internal governance and risk management (hereinafter "Circular CSSF 12/552") for investment firms and replaces it with Circular CSSF 20/758 on the central administration, internal governance and risk management (hereinafter "Circular CSSF 20/758"). Circular CSSF 12/552 shall remain applicable in its entirety to credit institutions and in part to professionals performing lending operations.

[1] *EBA/GL/2018/02 only aims at CRR investment firms.*

[2] *EBA/GL/2016/09 only aims at CRR investment firms.*

4. The guidelines referred to under point 2 have been incorporated into Circular CSSF 20/758. The terminology and definitions of the circular have also been reviewed and some provisions have been specified. A "track changes" version of Circular CSSF 12/552 and Circular CSSF 20/758 is included in Annex 1.

5. The main changes in relation to Circular CSSF 12/552 concern:
   a. extension of the scope to financial holding companies and mixed financial holding companies;
   b. specification of the concept of proportionality by linking it to the notion of systemic institution within the meaning of the Law of 5 April 1993 on the financial sector;
   c. clarifications regarding the application of proportionality when implementing the internal control functions;
   d. strengthening of the management body, in its supervisory function, via enhanced provisions with respect to diversity and independence;
   e. consideration of environmental, social and governance (ESG) risk factors with a view to ensuring viability of the business model.
   f. presentation of the main changes between Circular CSSF 12/552 and Circular CSSF 20/758 is included in Annex 2.

6. This Circular shall apply as from 1 January 2021.

Claude WAMPACH
Director

Marco ZWICK
Director

Jean-Pierre FABER
Director

Françoise KAUTHEN
Director

Claude MARX
Director General

Annexes :

Annex 1 : "Track changes" version of Circular CSSF 12/552 and Circular CSSF 20/758

Annex 2 : Presentation of the main changes between Circular CSSF 12/552 and Circular CSSF 20/758

Commission de Surveillance du Secteur Financier

The color code used for the "track changes" version is as follows:

- Red for addition/~~deletion~~
- Green for text movement

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

~~**Circular CSSF 12/552 as amended by Circulars CSSF 13/563, CSSF 14/597, CSSF 16/642, CSSF 16/647 and CSSF 17/655**~~

Circular CSSF 20/758

Re: Central administration, internal governance and risk management~~[1]~~

Luxembourg, ~~11~~7 December ~~2012~~ 2020

To all ~~credit institutions,~~ investment firms~~ and professionals performing lending operations~~[1]

Ladies and Gentlemen,

Articles ~~5~~ 17(1a) and ~~17 (1a)~~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")[2] require ~~credit institutions and~~ investment firms to have robust internal governance arrangements, which shall include a clear organisational structure with well-defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks to which they are or might be exposed~~to~~, adequate internal control mechanisms, including sound administrative and accounting procedures and remuneration policies and practices ~~that are consistent with~~allowing and ~~promote~~promoting sound and effective risk management, as well as control and security mechanisms ~~of~~for their IT systems.

~~[1] As regards professionals performing lending operations as defined in Article 28-4 of the law of 5 April 1993 on the financial sector, only Chapter 3 of Part III shall apply.~~

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

Commission de Surveillance du Secteur Financier

~~In~~This Circular specifies the ~~past, as a result~~ measures investment firms must take pursuant to the provisions of the ~~regulatory developments at~~ LFS and RCSSF 15-02[3] as regards central administration, internal governance and risk management. It reflects the European and international ~~level and the local needs, the CSSF specified~~ principles, guidelines and recommendations which apply in this respect, translating them, in a proportionate way, in the ~~procedures for implementing these articles in various circulars. The addition~~context of ~~new circulars transposing~~ the ~~guidelines~~ Luxembourg financial sector. Where, due to the size, the nature and the complexity of the activities and the organisation, the application of the principle of proportionality requires enhanced central administration, internal governance or risk management, the institutions shall refer to the principles set out in Chapter 2 of Part I and to the above-mentioned guidelines and recommendations for guidance on this implementation. This concerns especially the European Banking Authority ~~(~~("EBA~~) on internal governance of 27 September 2011 ("EBA")~~ Guidelines on internal governance (~~GL 44)"~~) and those of the Basel Committee on Banking ~~Supervision (BCBS)~~EBA/GL/2017/11) and the joint EBA and the European Securities and Markets Authority ("ESMA") Guidelines on the assessment of the suitability of members of the management body and key function holders (EBA/GL/2017/12).

This Circular repeals and replaces Circular CSSF 12/552 on ~~internal audit of 28 June 2012 ("The internal audit function in banks") would have resulted in significant redundancies and a multiplication of the terms used. Thus, the CSSF decided to bring together all the key implementing provisions on~~ **central administration, internal governance** ~~in one single circular. This circular reflects the above-mentioned EBA and BCBS guidelines supplementing them~~**and risk management (as amended by** ~~the additional provisions included in~~ **Circulars** ~~IML 96/126, IML 98/143~~**CSSF 13/563, CSSF** ~~04/155~~**14/597, CSSF** ~~05/178 and~~**16/642, CSSF** ~~10/466~~[4]**16/647, CSSF 17/655 and CSSF 20/750) with regard to investment firms.**

~~Furthermore, in order to provide an overview, this circular includes, by reference to Articles 5 (1) and 17 (1) of the law of 5 April 1993 on the financial sector, the implementing procedures on central administration as specified in Circular IML 95/120.~~

[3] *Idem*

[4] ~~*Circulars IML 96/126 regarding the administrative and accounting organisation, IML 98/143 regarding the internal control, CSSF 04/155 regarding the Compliance function, CSSF 05/178 regarding the administrative and accounting organisation; outsourcing of IT services and CSSF 10/466 regarding disclosures in times of stress.*~~

Commission de Surveillance du Secteur Financier

~~Consequently, Circulars IML 95/120, IML 96/126, IML 98/143, CSSF 04/155, CSSF 05/178 and CSSF 10/466 shall be repealed for credit institutions and investment firms.[5]~~

~~Finally, the purpose of this circular is also to gather all the provisions on risk management.~~

~~This circular represents a first step on the way to a consolidated regulatory collection in respect of internal governance in a broad sense. It does not include all the targeted areas, such as for example remuneration which is covered by the CRD standards ("Capital Requirements Directive" - Circulars CSSF 06/273 and CSSF 07/290) and by Circular CSSF 11/505 providing details on the principle of proportionality as regards remuneration.~~

~~The same applies to risk. This circular essentially transposes the CEBS guidelines and the EBA guidelines dated 2 September 2010 on concentration risk ("CEBS Guidelines on the management of concentration risk under the supervisory review process (GL31)"), the guidelines dated 27 October 2010 on liquidity pricing ("Guidelines on Liquidity Cost Benefit Allocation"), the EBA guidelines of 22 May 2015 on the management of interest rate risk arising from non-trading activities (EBA/GL/2015/08) and the EBA guidelines of 14 December 2015 relating to the 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). Moreover, the circular highlights the basic principles of prudence in the field of credit granting and private wealth management.~~

~~As far as CRR institutions[6] are concerned~~As regards the appointments of directors, authorised managers and key function holders, this Circular ~~shall~~should be read in conjunction with ~~CSSF Regulation N° 15-02 relating to the supervisory review and evaluation process that applies to CRR institutions~~the Prudential Procedure in this respect published on the CSSF website.

~~The various existing circulars relating to risks and their management will be brought together in a subsequent version of this circular.~~

~~Where, as a result of international regulatory developments or local needs, the CSSF is called upon to specify the requirements in this circular, it will update this circular. Part IV of the circular includes a chronology of the updates which enables the reader to track the changes operated by the successive updates.~~

~~*[5] Circulars IML 95/120, IML 96/126, IML 98/143 shall remain applicable for PFS other than investment firms, as well as Circular CSSF 17/656 which repeals and replaces Circular CSSF 05/178. These circulars together with Circular CSSF 04/155 shall remain applicable for payment institutions and electronic money institutions.*~~

~~*[6] The term "CRR institution" is defined in Article 1(1) of CSSF Regulation N° 15-02.*~~

The Circular is divided into four parts: the first part contains definitions and establishes the scope, the second part is dedicated to ~~the~~ 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 transitional measures and repealing provisions. The table of contents is as follows~~of this Circular.

~~The boxes which appear in the circular include the remarks and clarifications which serve as guidance to update the requirements included in this circular.~~

~~TABLE DES MATIÈRES /~~ TABLE OF CONTENTS

Part I - Definitions and Scope

Chapter 1. Definitions and abbreviations

~~**Part I. Definitions and scope**~~

~~**Chapter 1. Definitions**~~

1. For the purposes of this Circular:

1) ~~"~~"Board of Directors~~"~~" shall mean the body or, failing that, the persons who, under company law, monitor the management by the authorised management. ~~The term is~~ According to the financial sector regulation, Boards of Directors of investment firms are assigned responsibilities as regards the supervision and control, as well as the determination and approval of strategies and key policies. The term "Board of Directors" shall not ~~to~~ be understood in its legal sense as ~~banks and~~ investment firms can also take a legal form which does not provide for a ~~"~~"Board of Directors~~"~~" within the meaning of company law. For instance, ~~when there is~~ in a two-tier structure, the Board of Supervisors~~, the latter~~ shall assume the responsibilities that this Circular assigns to the ~~"board of directors";~~"Board of Directors". The Board of Directors shall also correspond to the management body, in its supervisory function, according to EBA/GL/2017/11.

2) ~~"~~"authorised management~~"~~" or "authorised managers" shall mean the persons referred to in ~~Articles 7~~ Article 19(2) ~~and 19~~ of the LFS. From a prudential standpoint, the authorised management shall be in charge of the day-to-day management of an investment firm, in accordance with the strategic directions and the key policies approved by the Board of Directors. The authorised management shall also be considered as the management body, in its management function, according to EBA/GL/2017/11.

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

~~2)~~3) "CRR investment firm" shall mean an investment firm within the meaning of point (2) of ~~the law of 5 April 1993 on the financial sector. These persons are referred to as "authorised managers";~~Article 4(1) of Regulation (EU) No 575/2013.

4) ~~"institution"~~"non-CRR investment firm" shall mean an ~~entity~~investment firm other than a CRR investment firm.

~~3)~~5) " "institution(s)" or "investment firm(s)" " shall mean CRR and non-CRR investment firms incorporated under Luxembourg law, including their branches and the Luxembourg branches of third-country investment firms, as ~~defined~~well as Luxembourg branches of investment firms authorised in ~~Chapter 2 of Part I;~~another Member State.

6) ~~"key function": any function the exercise of which may have~~"significant institution" shall, for the purposes of this Circular, mean a systemically important investment firm in accordance with Article 59-3 of the LFS and, if applicable, other investment firms determined as such by the CSSF based on the assessment of the investment firms' size and internal organisation as well as the nature, the scale and the complexity of their activities.

7) "ICAAP" shall mean Internal Capital Adequacy Assessment Process.

8) "ILAAP" shall mean Internal Liquidity Adequacy Assessment Process.

9) "LFS" shall mean the Law of 5 April 1993 on the financial sector, as amended.

10) "MiFID" shall mean the Markets in Financial Instruments Directive.

11) "management body" shall mean the management body, in accordance with the definition of the LFS, and shall be the management body in its supervisory function and in its management function in accordance with EBA/GL/2017/11. It shall refer to the Board of Directors and the authorised management of an institution with a one-tier structure or the Supervisory Board and the Executive Board of an institution with a two-tier structure.

12) "related parties" shall mean the legal entities (structures) which are part of the group to which the institution belongs as well as the staff members, shareholders, managers and members of the Board of Directors of these entities.

13) "Prudential Procedure" shall mean the prudential procedure for the approval of directors, authorised managers and key function holders in investment firms.

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

~~4)~~15) "key function holders" shall mean the heads of functions whose performance allows a significant influence ~~on~~over the conduct or monitoring of the activities~~. These key functions~~ of the institutions. They include~~ at least~~, in particular, the ~~directors, authorised managers and the persons in charge~~heads of the three internal control functions in ~~accordance with point 105 (~~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.

~~1) "LFS" shall mean the law of 5 April 1993 on the financial sector;~~

~~2) "related parties" shall mean the legal entities which are part of the group to which the institution belongs as well as the employees, shareholders, managers and members of the board of directors of these entities.~~

Chapter 2. Scope and proportionality

2. This Circular shall apply to ~~credit institutions and~~ investment firms ~~governed by~~incorporated under Luxembourg law, including their branches, as well as the Luxembourg branches of ~~credit institutions and~~third-country investment firms ~~originating outside the European Economic Area.~~.

In respect of the areas for which the CSSF retains an oversight responsibility as host authority – i.e. ~~measures in the fight against~~ anti-money laundering and counter terrorist financing~~, markets in financial instruments~~ measures and ~~liquidity~~rules applicable to the provision of investment services – Luxembourg branches of ~~credit institutions and~~ investment firms ~~originating from a~~authorised in another Member State ~~of the European Economic Area~~, in coordination with this authorised firm, shall establish central administration ~~and~~, internal governance ~~arrangements as well as~~ and risk management arrangements which are comparable to those provided for in this Circular.

~~All entities mentioned in the preceding paragraphs are referred to hereafter as "institutions".~~

~~In respect of professionals performing lending operations as defined in Article 28-4 of the LFS, only Chapter 3 of Part III of this~~ This Circular shall apply~~.~~

~~Chapter 6 of Part III of this circular applies only to credit~~ to institutions~~.~~

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

~~Where there are legal entities, whether consolidated or not, whose~~ If the institution is a parent undertaking ~~is the institution within the meaning of the LFS, the term "institution" shall refer to the "group", i.e. the entire group represented by the parent undertaking (the "group head") and the legal entities whose parent undertaking is the institution within the meaning of the LFS.~~(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 ~~it,~~this group - whether or not they are included in the scope of prudential consolidation according to the CRR - including ~~their possible~~the branches~~, as well as the relationships between these legal entities~~, in compliance with the national laws and regulatory provisions which apply to the ~~legal~~ entities in question.

~~In the case of legal entities in which the institution holds an interest of between 20% and 50% but whose parent undertaking is not the institution within the meaning of the LFS, the institution - group head - together with the other shareholders or partners concerned shall do their utmost to make sure that central administration and internal governance arrangements as well as risk management arrangements are implemented within these legal entities. These arrangements shall meet standards which are comparable to those provided for in this circular and comply with the laws and regulatory provisions applicable at national level.~~

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

~~2.~~ Proportionality shall apply to the implementing measures, which the institutions take pursuant to this Circular, having regard to the nature, scale and complexity of ~~the~~their activities, including the risks ~~and organisation of the institution.~~

. In practice, the application of the principle of proportionality implies that the ~~largest, most complex or riskiest~~ institutions ~~shall~~which are more significant, complex or riskier have in place enhanced central administration ~~and~~, internal governance and risk management arrangements. These enhanced arrangements shall include, for example, the establishment of specialised committees ~~pursuant~~, the appointment of independent members additional to ~~Section 4.1.4. However, for institutions whose activity is less diversified, significant~~the Board of Directors or ~~complex~~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 ~~less strictly.~~downward. Thus, ~~these institutions~~an institution with limited activities of low complexity may operate properly within the meaning of this Circular ~~with~~ by designating heads of compliance and risk control functions ~~assumed~~ on a part-time basis (~~cf. points 129 and 141), with an outsourced~~ 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 ~~(point 117) or through the use of external experts in order to carry out some internal control tasks (point 118).~~. The ~~less stringent~~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~~must be assigned so as to avoid conflicts of interest involving the same person ~~(cf. point 71). At the level of the authorised management, this principle is balanced with the principle of overall responsibility of the authorised management (cf. point 72).~~ .

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

The implementation of the principle of proportionality~~, where an~~ shall take account of the following:

a. the legal form and the ownership and funding structure of the institution ~~does not require more than two authorised managers, the effective division of duties is not always compatible with a strict segregation of duties within this management. For instance, in this case, the same member of the authorised management may be in charge of both the administrative, accounting and IT organisation and the internal control functions (cf. point 63).~~ ;
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 ~~organisation~~ adopted organisation, the arrangements in this respect shall enable the institution to operate in full compliance with the provisions of ~~Chapter 3 of Part II.~~ Part II of this Circular. The institutions shall document their proportionality analysis in writing and have their conclusions approved by the Board of Directors.

Part II. Central administration and internal governance arrangements

Chapter 1. Central administration

1. The institutions shall have a robust central administration in Luxembourg, consisting of ~~a "~~their "decision-making centre~~"~~" and ~~an "~~their "administrative centre~~".~~". The central administration, which ~~comprises~~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 ~~concept of "~~decision-making centre~~" does not only comprise~~ shall include the authorised ~~management's activities pursuant to Articles 7 (2)~~management and ~~19 (2) of~~ the ~~LFS but also that~~heads of the ~~persons in charge of the various~~ business~~,~~ functions, the support and control functions ~~or~~and the various business units ~~(services, departments or positions)~~ existing within the institution.

3. The administrative centre shall include ~~in particular a sound~~the administrative, accounting and IT organisation which ~~ensures~~shall ensure, at all times, proper administration of securities and assets, ~~proper~~adequate execution of operations, accurate and complete recording of operations and production of accurate, complete, relevant and understandable management information available without delay. ~~In this respect, it shall include the administrative infrastructure of the business functions (Section 5.2.1), the support functions, in particular in the financial and accounting field (Section 5.2.2) and the IT field (Section 5.2.3) as well as the internal control (Chapter 6).~~

4. Where the institution is the group head ~~pursuant to point 3~~, the central administration shall enable the institution to concentrate ~~all~~any management information necessary to manage, monitor and control ~~, on an ongoing basis,~~ the activities of the group ~~in~~, on an ongoing basis, within its ~~registered~~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 ~~required~~necessary management information. The concept of management information shall be understood in the broadest possible sense, including financial information and ~~the prudential~~legal reporting.

Chapter 2. Internal governance arrangements

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

Internal governance ~~shall~~must ensure ~~in particular~~ a sound and prudent ~~business~~ management of the activities, including ~~the risks~~of inherent ~~in them. In order to achieve this objective, the institutions shall establish~~ risks. The internal governance arrangements ~~which are consistent with the three lines of defence model.~~

~~The first line of defence consists of the business units that take or acquire risks under a predefined policy and limits and carry out controls as described under Section 6.1.1.~~

~~The second line is formed by the support functions, including the financial and accounting function (Section 5.2.2) as well as the IT function (Section 5.2.3), and the compliance and risk control functions (Sub-chapter 6.2 and Sections 6.2.5 and 6.2.6) which contribute to the independent risk control.~~

~~The third line consists of the internal audit function which, pursuant to Sub-chapter 6.2 and Section 6.2.7, provides an independent, objective and critical review of the first two lines of defence.~~

6. ~~The three lines of defence are complementary, each line of defence assuming its control responsibilities regardless of the other lines.~~ ~~The controls carried out by the three lines of defence~~ shall include ~~the four levels of control provided for in point 100.~~:

~~3. In essence, and for the purpose of complying with the objectives laid down in the preceding point, the internal governance arrangements shall include in particular:~~

- a clear and consistent organisational and operational structure ~~including~~with decision-making powers, reporting and functional ~~links~~lines and ~~segregation~~share of ~~duties~~responsibility which are ~~clearly~~ well-defined, transparent, consistent, complete and free from conflicts of interest ~~(Sub-chapters 5.1, 7.1 and 7.2);~~;
- 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 ~~by applying the rules laid down in Circulars CSSF 06/273, CSSF 07/290 and CSSF 11/505~~, in line with the institution's risk strategy, as well as control and security mechanisms for ~~the~~ management information systems. The concept of management information system shall include ~~the information~~IT systems ~~(Sections 5.2.1 to 5.2.3, Sub-chapters 5.3 and 7.4);~~;
- 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~~, where appropriate,~~ sanction procedure for the problems, shortcomings and irregularities identified through the internal control ~~mechanisms, including the internal control functions under Sub-chapter 6.2~~and alert mechanisms;

- ~~processes to identify, measure, report, manage and mitigate as well as monitor the risks institutions are or may be exposed to pursuant to Chapter 1 of Part III;~~
- ~~a management information system, including as regards risks, as well as internal communication arrangements including internal whistleblower procedure which enables the staff of the institution to draw the attention of those responsible to all their significant and legitimate concerns related to the internal governance of the institution (Section 5.2.4);~~
- business continuity management arrangements aimed to limit the risks of ~~serious~~ severe business disruption ~~of business activities~~ and to maintain the key operations as defined by the Board of Directors upon proposal of the authorised management. These arrangements shall include a business continuity plan which describes the actions to be ~~put in place~~taken in order to continue to operate in case of an incident or disaster ~~(Sections 5.2.3 and 7.4);~~ ;
- crisis management arrangements which ensure appropriate responsiveness in ~~case~~the event of a crisis, including a ~~business~~ recovery plan~~. These arrangements shall meet~~ in accordance with the requirements ~~set out in Section 5.~~of Chapter 2~~.5~~ of Part IV of the LFS.

7. ~~The institutions~~Any institution shall promote an internal risk and ~~control~~compliance culture in order to ensure that all the institution's staff ~~of the institution~~ 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 ~~as defined in Chapter 6~~.

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

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

8. Central administration and internal governance arrangements shall be developed and implemented so that they:
   - ~~fully~~ 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, institutionsany 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 controlled; 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 itstheir parts ("(“consistency");”);
- are comprehensive ("(“comprehensiveness").”). In respect of riskrisks, comprehensiveness shall mean that all risks shallmust be included within the scope of the internal governance arrangements. This scope isshall not (necessarily)be limited to the sole (consolidated) prudential or accounting scope; it. This scope shall enable the institution to have a thorough overview of all its risks, in terms of their economic substance, taking into accountconsidering 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.;

4. In application of an organisation chart (Sub-chapter 5.1), the institution shall have in its registered office in Luxembourg, in its branches as well as all in the different legal entities which are part of the group, a sufficient number of human resources with appropriate individual and collective professional skills as well as the necessary and sufficient administrative and technical infrastructure to carry out the activities which it wishes to perform. These human resources and this infrastructure shall comply with the provisions of Sub-chapters 5.1 and 5.2.

Outsourcing is possible under the conditions laid down in Sub-chapter 7.4.

5. Institutions shall set out in writing all the central administration and internal governance arrangements as well as all their activities (operations and risks) pursuant to Sub-chapter 5.3.

- comply with the legal and regulatory requirements, including with the requirements of this Circular (“compliance”).

9. In order to ensure and maintain the soundnessrobustness 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 shouldshall consider all internal and external changes which may have a significant adverse effect on the soundnessrobustness 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. ~~Institutions~~The CRR investment firms shall ~~publish~~disclose the key elements ~~of their~~on internal governance ~~arrangements~~and risk management in ~~compliance~~accordance with the ~~rules governing Part XIX of Circular CSSF 06/273 ("Pillar 3"). This publication shall comprise~~ provisions of the ~~organisational and operational structure, including as regards the internal control, risk strategy as well as risk profile. This information shall describe the current situation~~CRR (Article 435 and ~~its expected development in a clear, objective~~Title I of Part Eight) and ~~relevant manner.~~ the EBA Guidelines on disclosure requirements under Part Eight of Regulation (EU) No 575/2013 ("EBA/GL/2016/11").

Chapter 4. Board of Directors and authorised management

Sub-chapter 4.1. Board of Directors

Section 4.1.1. Responsibilities of the Board of Directors

11. The Board of Directors shall have the overall responsibility for the institution. It shall ~~ensure execution of activities~~define, monitor and ~~preserve business continuity by way of sound~~ bear responsibility for the implementation of robust central administration, governance and internal ~~governance~~control arrangements ~~pursuant to the provisions of this circular. To this end, in compliance with the legal and regulatory provisions and~~, 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 ~~persons in charge~~heads of the internal control~~, and for the purpose of protecting the institution and its reputation~~ functions, the Board of Directors shall approve and lay down, in writing, ~~notably~~ the following key elements of the central administration, internal governance and risk management arrangements:

- ~~the~~ the business strategy (business model) of the institution ~~taking into account~~, considering the institution's long-term financial interests, solvency ~~and~~, liquidity situation~~;~~
- ~~the institution's risk strategy~~ and risk appetite. The development and maintenance of a sustainable business model requires that account be taken of all material risks, including ~~the risk tolerance and the guiding principles governing the risk identification, measurement, reporting, management and monitoring~~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 ~~own funds~~capital and liquidity reserves;
- ~~the guiding principles of~~ a clear and consistent organisational and operational structure which ~~governs~~shall govern, in particular, the creation and maintenance of legal entities (structures) by the institution ~~as well as~~;
- the guiding principles as regards information systems, ~~including the~~ technology and security ~~aspect, and~~in accordance with Circular CSSF 20/750, including the internal communication and alert arrangements~~, including the internal whistleblower procedure~~;
- the guiding principles relating to the internal control mechanisms, including the internal control functions ~~and remuneration policy,~~ ;
- the guiding principles ~~for~~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~~, settlement~~ and sanctions the purpose of which is to ensure that any behaviour which does not comply with the applicable rules ~~shall be~~is properly investigated and sanctioned~~, as well as the guiding principles of professional conduct ("internal code of conduct") and corporate values, including as regards the management of conflicts of interest~~;
- the guiding principles ~~as regards~~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~~, the guiding principles as regards the administrative, accounting and IT organisation, the guiding principles as regards outsourcing, including IT-related outsourcing relying on a cloud computing infrastructure or not, as well as the guiding principles governing the change in activity (in terms of coverage of markets and customers, new products and services) and the approval and maintenance of "non-standard" or "non-transparent" activities;~~;
  - an administrative, accounting and IT organisation with integrity, and complying with the applicable laws and standards;
  - the guiding principles ~~applicable~~ relating to outsourcing, including IT-related outsourcing, whether or not it is based on a cloud computing infrastructure, and

- o 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 ~~management~~ and crisis management ~~arrangements~~, and
- the guiding principles ~~on~~governing the appointment and succession to the Board of ~~individuals with~~Directors, the authorised management and key ~~functions~~function holders in the institution, as well as the procedures governing the composition of the Board of Directors, including the aspects of diversity, responsibilities, organisation ~~and~~, operation ~~of the board of directors~~, and individual and collective assessment of its members.[7] The ~~guiding principles governing the appointment and succession of individuals with key functions in the institution provide that, in this regard, the institution~~aspects of diversity shall ~~comply with the requirements of this circular, the prudential authorisation procedure of key function holders as published on the CSSF's website as well as the guidelines published by the EBA on 22 November 2012 (Guidelines on~~ refer to the ~~assessment~~characteristics of the ~~suitability of~~ members of the management body ~~and key function holders – EBA/GL/2012/06).~~, 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.

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

~~**Comment:**~~

~~The EBA guidelines on the assessment of the suitability of the key function holders provide in particular that the institutions shall:~~

- ~~identify all key functions (cf. also point 1 in this regard);~~
- ~~define the criteria (in terms of professional standing, professional skills and personal qualities) under which the key function holders are assessed. These criteria are consistent with the criteria provided for in points 13 to 15 of the aforementioned EBA guideline;~~
- ~~require that the key function holders are of good repute and have the professional skills and personal qualities required to fulfil their duties;~~
- ~~assess in writing the suitability of the key function holders, prior to their appointment, on a regular basis, during their mandate and on an ad hoc basis where such an assessment is imposed;~~
- ~~define policies and procedures for selecting key function holders who comply with the principles of robust internal governance (in accordance with points 7 and 8 of the aforementioned EBA guidelines.~~

12. The Board of Directors shall entrust the authorised management with the implementation of the ~~internal governance~~ strategies and guiding principles ~~referred to in point 17~~ through ~~the~~ internal written policies and procedures~~,~~ (except for the guiding principles governing the appointment and succession ~~of individuals to~~within the Board of Directors~~.~~ and the procedures determining its operation).

13. The Board of Directors shall monitor the implementation by the authorised management of ~~its internal governance~~ the strategies and guiding principles~~. To this end, it shall in particular~~ and approve the policies ~~laid down~~established by the authorised management ~~pursuant to point 18.~~ according to these strategies and principles.

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

The assessment and re-approval by the Board of Directors shall relate, in particular, ~~assess and approve:~~

~~the adequacy of~~ to the ~~risks~~ following:

- the correlation between the incurred ~~with~~risks, the institution's ability to manage these risks and the internal and regulatory ~~own funds~~capital and liquidity reserves, ~~taking into account~~in line with the strategies and guiding principles ~~laid down~~established by the Board of Directors~~,~~ and the ~~existing~~applicable regulations ~~and in particular~~, 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 ~~the~~its responsibilities ~~set out in Sub-chapter 4.2.~~and the performance of its members. In this context, the Board of Directors shall ~~ensure~~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 ~~effectively~~efficiently implements the ~~required~~ 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 CSSF~~, pursuant to the last two paragraphs of point 57~~ and, where applicable, another competent authority;
- the adequacy of the organisational and operational structure. The Board of Directors ~~shall~~must fully know and understand the organisational structure of the institution, in particular ~~in terms~~ of the underlying legal entities (structures), ~~of~~ their raison d'être, the intra-group links and ~~interconnections between them~~interactions as well as the risks related thereto. It shall verify that the organisational and operational structure complies with the strategies and guiding principles ~~referred to in point 17~~, 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 ~~set~~assigned objectives. This requirement shall apply, in particular, to ~~"~~non-standard~~"~~ or ~~"~~potentially non-transparent~~"~~ activities;
- the ~~efficiency and~~ effectiveness and efficiency of the internal control mechanisms put in place by the authorised management.

The assessments in question may be prepared by ~~the~~specialised committees ~~established in accordance with point 33~~. These assessments shall, in particular, be based on the information received from the authorised management ~~(point 61),~~, the audit reports issued by the *réviseur d'entreprises agréé* (reports on ~~the~~ annual accounts, long ~~-~~form reports and, where appropriate, ~~the~~ management letters), the ICAAP ~~report (point 61) and the summary~~/ILAAP reports and the reports of the internal control functions ~~(point 116)~~ which the Board of Directors is called upon to approve on this occasion.

15. The Board of Directors ~~is~~shall be in charge of promoting an internal risk and compliance culture which ~~heightens~~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 ~~vis-à-vis~~towards internal control and compliance. It shall also be in charge of stimulating the development of ~~the~~ internal governance arrangements which allow reaching these objectives.

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

16. The Board of Directors ~~approves the internal audit plan pursuant~~shall ensure that sufficient time is devoted to ~~point 151~~risk issues.

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

Section 4.1.2. Composition and qualification of the Board of Directors

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

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

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

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

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

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

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

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

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

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

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

Section 4.1.3. Organisation and functioning of the Board of Directors

~~23.~~24. The Board of Directors shall regularly meet ~~on a regular basis~~ in order to effectively ~~perform~~fulfil its ~~duties~~responsibilities. The organisation and functioning of the Board of Directors shall be documented in writing. The objectives and responsibilities of its members shall also be documented by way of written mandates.

~~24.~~25. The work of the Board of Directors ~~shall~~must be documented in writing. This documentation shall include the agenda ~~of the meeting, the~~ and minutes of the ~~meeting~~meetings as well as the decisions and measures taken by the Board of Directors. The minutes are an important tool which must, on the one hand, help the Board of Directors and its members monitor the decisions and, on the other hand, enable the Board of Directors and its members to be accountable to the shareholders and the CSSF. Thus, the routine items may be included succinctly in the minutes of a meeting, in the form of a simple decision, while important items on the agenda involving risks for the institution or jointly discussed must be reported in more detail, allowing readers to follow the discussions and to identify the positions taken.

~~6.~~ The Board of Directors shall assess~~, on a regular basis,~~ the procedures governing ~~the board of directors, its~~its operating mode ~~of functioning~~ 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.

26. ~~The chairman of the board of directors is in charge of promoting,~~It shall ensure that all its members have a clear picture of their obligations, responsibilities and allocation of tasks within the Board of Directors~~,~~ and specialised committees that depend on it.

~~7.~~ The chairperson of the Board of Directors shall ensure a balanced composition thereof, in particular in terms of diversity, to ensure its proper functioning, to promote a culture of informed ~~and contradictory~~ discussion in which all parties are heard within the Board of Directors and to propose the ~~election~~appointment of independent directors. ~~An independent director~~The chairperson of the Board of Directors shall ~~be a director who does~~ not ~~have any conflict of interest which might impair his/her judgement because s/he is bound by a business – family or other[8] – relationship with~~exercise executive functions within the institution~~, its controlling shareholder or the management of either.~~

~~The CSSF recommends larger institutions to have one or several independent directors.~~

~~25.~~27. . Thus, the mandates of authorised manager and ~~chairman~~chairperson of the Board of Directors cannot be combined and the chairperson of the Board of Directors cannot be another staff member of the institution.

~~[8] Including an employment relationship.~~

Commission de Surveillance du Secteur Financier

Section 4.1.4. Specialised committees

28. ~~For the purpose of increasing its effectiveness,~~ The Board of Directors may be assisted by specialised committees ~~notably~~, in particular, in the fields of ~~auditing, risk~~audit, risks, compliance, remuneration~~, human resources (notably through the intervention of a nomination committee of the key function holders) as well as~~ and appointments or internal governance~~,~~ and professional ethics, according to its needs and ~~compliance where~~considering the organisation, nature, scale and complexity ~~of the institution and its activities so require. These committees shall include directors who are not members either of the authorised management or~~ of the institution's ~~staff. They may also include, if need be, external independent experts of the institution. Their mission is~~ activities. The missions of the specialised committees shall be to provide the Board of Directors with critical assessments in respect of the organisation and ~~operation~~functioning of the institution in ~~the aforementioned~~their specific areas ~~in order to enable~~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 ~~board of directors~~necessary knowledge, skills and expertise to perform their functions, both individually and collectively.

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

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

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

~~26.~~34. The specialised committees shall meet on a regular basis in order to discharge their tasks and work assigned to them or to prepare the meetings of the Board of Directors. According to their needs, they may be assisted by external experts independent of the institution, and may involve, in their work, the *réviseur d'entreprises agréé*, the authorised managers, the other specialised committees, the heads of the internal control functions and the other persons working for the institution, provided that these persons are not members and do not take ~~on their responsibilities pursuant to this circular.~~part in the recommendations of the committee.

~~27.~~35. The Board of Directors shall lay down, in writing~~:~~, the ~~mandate~~missions, composition and working procedures of the specialised committees. ~~Pursuant to~~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. ~~Moreover, the~~ 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 ~~*réviseur d'entreprises agréé* as well as any person belonging to the institution, including the authorised management, are associated with~~external experts provide their assistance and the terms under which other persons are involved in the work of the specialised committees.

~~28.~~36. The Board of Directors shall ensure that the ~~various~~different committees interact effectively ~~interact~~, communicate with each other, with the internal control functions and the *réviseur d'entreprises agréé*, and report to the Board of Directors on a regular basis.

~~8.~~ The Board of Directors cannot delegate its ~~decision-making~~ powers and responsibilities ~~to specialised committees~~ pursuant to this Circular~~.~~

~~9. The specialised committees are chaired by one of their members. These committee chairmen shall have in-depth knowledge in the area of activities of the committee they chair.~~

~~29.~~37. to the specialised committees. Where the Board of Directors is not assisted by specialised committees, the tasks referred to in Sub-sections 4.1.4.1 and 4.1.4.2 shall be directly incumbent upon the Board of Directors.

Sub-section 4.1.4.1. Audit committee[9]

~~30.~~38. The purpose of the audit committee ~~is~~shall be to assist the Board of Directors in the areas of financial information, internal control, including internal audit as well as the ~~control~~audit by the *réviseur d'entreprises agréé*.

~~10. The CSSF recommends larger~~ Without prejudice to the other provisions of Section 4.1.4, the institutions ~~to~~must establish an audit committee ~~in order to facilitate effective supervision of the activities~~when imposed by ~~the board of directors.~~

~~31.~~39. ~~The audit committee shall comprise at least three members and its composition shall be determined in accordance with its missions and its mandate pursuant to points 33 and 34. The collective competences~~Article 52 of the ~~members of~~Law of 23 July 2016 concerning the audit ~~committee shall be representative of the activities and risks of the institution and include specific competences regarding audit and accounting. The audit committee can involve the person in charge of the internal audit function as well as the *réviseur d'entreprises agréé* of the institution in the work of the authorised management. These persons can attend the committee's meetings; they are not members of it.~~profession, as amended ("Audit Law").

~~32.~~40. ~~The functioning of~~ The audit committee~~, in particular in terms~~ shall be in charge of the process of ~~frequency~~appointment, reappointment, revocation[10] and ~~duration~~remuneration of the ~~meetings, shall be determined in relation to its mandate and its mission to assist the board of directors.~~ *réviseur d'entreprises agréé*.

~~33.~~41. The audit committee shall confirm the internal audit charter ~~(point 144).~~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 ~~(point 111)~~ and ~~that the~~ independence ~~of the internal audit function is safeguarded~~.

~~11. The audit committee shall confirm the internal audit plan (point 151) confirmed by the authorised management. It shall take note of the information on the state of the internal control provided by the authorised management at least once a year pursuant to point 61 of this circular.~~

~~12. The audit committee shall deliberate, on a regular basis, on~~[11]~~:~~

~~[9] In respect of institutions which shall have an audit committee pursuant to the law of 18 December 2009 concerning the audit profession, this circular shall apply without prejudice to the codified provisions of Article 74 ("Audit Committee") of this law.~~

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

~~[11] Annex 2 of the BCBS guidelines on the internal audit function in banks dated 28 June 2012 includes a more comprehensive list of tasks generally assigned to the audit committee.~~

42. ~~the follow-up of~~ The audit committee shall regularly and critically deliberate on the following[12]:

- the compliance with the accounting rules and the financial reporting process;
- the state of the internal ~~audit~~control and the compliance with the rules set in this respect in this Circular ~~on the basis~~, 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 ~~in this circular (cf. Sections 6.2.3 and 6.2.7.3);~~

- ~~the appointment, renewal, revocation and remuneration of the *réviseur d'entreprises agréé*~~;
- 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 ~~applicable to the audit area.~~as well as the scope and frequency of the audits. In this respect, the audit committee shall ~~critically~~ analyse and assess the ~~audit plan, 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 annual accounts, the management letters as well as the long-form reports drafted by the *réviseur d'entreprises agréé* and shall examine and monitor the independence of the *réviseur d'entreprises agréé* or the *cabinet de révision agréé* (approved audit firm), in particular, in respect of the provision of additional services to the institution;~~

~~•~~ the appropriate and timely follow-up ~~without undue delay~~ by the authorised management of the recommendations of the internal audit function and the *réviseur d'entreprises agréé* ~~aimed to improve the organisation and internal control;~~

- and the actions taken to address the identified problems, shortcomings and irregularities.

~~•~~ When reporting to the Board of Directors as a whole, the audit committee shall propose the necessary measures to ~~be taken in case of~~promptly address the identified problems, shortcomings and irregularities ~~identified by the internal audit department and the *réviseur d'entreprises agréé*;~~

~~• the compliance with the legal and statutory provisions as well as with the CSSF rules for the drafting of the individual and, where appropriate, consolidated annual accounts, and on the relevance of the accounting policies adopted.~~

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

~~34.~~43. ~~The audit committee may also be in charge of the compliance function without creating a separate compliance committee. In this case, the mandate and the composition of~~. The audit committee shall ~~reflect these new tasks. In particular, the persons associated with the audit committee pursuant to point 39 shall include the Chief Compliance Officer pursuant to point 105.~~ inform the Board of Directors of the conclusions of the external audit, of its work to ensure the integrity of the legal reporting and of its role in this process.

Sub-section 4.1.4.2. Risk committee

~~35.~~44. The purpose of the risk committee ~~is~~shall be to ~~assist~~advise the Board of Directors ~~in its mission~~on aspects related to ~~assess~~ the ~~adequacy~~overall risk and risk appetite strategy and also to assist it in assessing the correlation between the ~~risks~~ incurred risks, the institution's ability to manage these risks, and the internal and regulatory ~~own funds~~capital and liquidity reserves.

~~13.~~ The ~~CSSF recommends larger~~significant institutions ~~as well as institutions with a higher or more complex risk profile to create~~must establish a risk committee in ~~order to facilitate~~ accordance with the ~~effective risk control by the board~~provisions of ~~directors.~~

~~36.~~45. ~~The risk committee can involve the authorised management as well as the persons in charge~~Article 7 of ~~the internal control in its work. These persons can attend the committee's meetings; they are not members of it~~RCSSF 15-02.

~~37.~~46. The risk committee shall confirm the specific policies of the authorised management in accordance with Section ~~4.2.3~~1.1.2 of Part III. It shall assist the Board of Directors in its supervisory mission, i.e. implementing the risk strategy, the overall risk-taking and risk management framework and the adequacy of all the incurred risks relating to the strategy, the risk appetite and the risk mitigation measures of the institution.

~~38.~~47. The risk committee shall assess whether the human and material resources, as well as the organisation of the risk control function ~~(Section 6.2.5)~~ are sufficient and shall ensure that the members of the risk control function have the required skills.

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

49. The risk committee shall regularly and critically deliberate~~,~~ on the following:

- the risk profile of the institution, its development as a ~~regular~~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, ~~on:~~considering its internal and regulatory capital and liquidity reserves;
- the ~~state~~adequacy of the risk-taking and risk management ~~and compliance with~~framework in relation to the ~~prudential rules laid down in this respect~~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 ~~respect in this circular (cf. Section 6.2.3 and in particular Section 6.2.5);~~

~~• the risk situation, its future development and its adequacy with the risk strategy of the institution;~~

- ~~the adequacy of the risks incurred with the current and future institution's ability to manage these risks and the internal and regulatory own funds and liquidity reserves, taking into account the results of the stress tests in accordance with~~ Circular ~~CSSF 11/506;~~ ;
- 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 ~~without undue delay~~ by the authorised management of the recommendations of the risk control function~~;~~

- and the actions ~~to be~~ taken ~~in case of~~ to address the identified problems, shortcomings and irregularities ~~identified by the risk control function.~~ ;
- ~~The risk committee shall advise the board of directors on the definition~~the compliance and the pricing of the ~~overall~~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, ~~including~~ its ~~current and future risk tolerance~~internal and regulatory capital and liquidity reserves as well as its profitability.

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

~~39.~~50. The chairperson of the risk committee cannot be, at the same time, the chairperson of the Board of Directors or of any other specialised committee.

Commission de Surveillance du Secteur Financier

Sub-chapter 4.2. Authorised management

Section 4.2.1. Responsibilities of the authorised management

~~40.~~51. The authorised management ~~is~~shall be in charge of the effective, sound and prudent day-to-day ~~business~~ management of the activities (and inherent ~~risk) management.~~risks). This management shall be exercised in compliance with the strategies and guiding principles ~~laid down~~approved by the Board of Directors and the ~~existing~~applicable regulations, ~~taking into account~~by considering and safeguarding the institution's long-term financial interests, solvency and liquidity situation. ~~The decisions~~ The authorised management shall constructively and critically assess all the proposals, explanations and information submitted to it for decision. The authorised management shall document its decisions by way of minutes of meetings, which must, on the one hand, help it monitor the decisions and, on the other hand, enable it to account for its management to the Board of Directors and the CSSF. Thus, the routine items may be included succinctly in the minutes of a meeting, in the form of a simple decision, while important items on the agenda involving risks for the institution or jointly discussed must be reported in more detail, allowing readers to follow the discussions and to identify the positions taken ~~by the authorised management in these areas shall be duly documented.~~ .

~~41.~~52. Pursuant to ~~Articles 7 (2) and~~ Article 19(2) of the LFS, the members of the authorised management ~~shall~~must be authorised to ~~effectively~~ determine the business direction effectively. Consequently, where management decisions are taken by larger management committees ~~which are larger~~ rather than solely ~~the authorised management,~~by the authorised management ~~shall~~ , at least one member of the authorised management must be part of it and have a veto right.

~~42.~~53. The authorised management ~~shall~~must, in principle, be permanently on – site. Any exemption to this principle ~~shall~~must be authorised by the CSSF.

~~43.~~54. The authorised management shall implement, through ~~internal~~ written internal policies and procedures, all the strategies and guiding principles laid down by the Board of Directors in relation to central administration and internal governance, in compliance with the legal and regulatory provisions and after having heard the internal control functions. The policies shall include detailed measures to be implemented; the procedures shall be the work instructions which govern this implementation. The term ~~"~~"procedures~~"~~" is to be taken in the broad sense, including all the measures, instructions and rules governing the organisation and internal functioning.

~~It~~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 ~~business~~management of the activities (and inherent ~~risk) management~~ risks) within the context of robust internal governance arrangements pursuant to this Circular.

55. ~~Pursuant to point 18~~Under the guiding principles of professional conduct, corporate values and management of conflicts of interest laid down by the Board of Directors, the authorised management shall define an internal code of conduct applicable to all the persons working in the institution. It shall ensure its ~~correct~~proper application on the basis of regular controls carried out by the compliance and internal audit functions.

~~14.~~ 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 ~~a regular basis.~~

it or legal disputes, the damage to its corporate image or the loss of the trust of its customers and the consumers. The code of conduct should remind the staff, the authorised managers and the members of the Board of Directors of the compliance with the applicable regulations, the internal rules and limitations, the principles that underlie honesty and integrity in their behaviour as well as the cases of inappropriate conduct and the sanction measures arising therefrom.

~~44.~~56. The authorised management ~~shall~~must have ~~an absolute~~a full understanding of the organisational and operational structure of the institution, in particular, ~~in terms~~ of the underlying legal entities (structures), of their raison d'être, the intra-group links and ~~interconnections between them~~interactions as well as the ~~risks~~ related ~~thereto~~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.

~~45.~~57. In its day-to-day management, the authorised management shall ~~take into account~~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~~, where appropriate,~~ of the compliance function.

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

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

~~46.~~58. The authorised management shall verify the implementation of and compliance with internal policies and procedures. Any ~~violation~~breach of internal policies and procedures shall result in prompt and adapted corrective measures.

~~47.~~59. The authorised management shall verify the ~~soundness~~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.

~~48.~~60. The authorised management shall inform the internal control functions of any ~~significant changes~~major change in the activities ~~(cf. Sub-chapter 7.3)~~ or organisation in order to enable them to identify and assess the risks which may arise therefrom.

61. The authorised management shall regularly or at least annually inform the Board of Directors, in a comprehensive manner and in writing, ~~on a regular basis and at least once a year, the board of directors~~ of the implementation, adequacy, effectiveness of and compliance with the internal governance arrangements, ~~including~~comprising the state of compliance ~~and~~ (including the concerns raised through the internal alert arrangements) and of internal control as well as the ICAAP ~~report~~[13]/ILAAP reports on the situation and the management of ~~the~~ risks ~~and the~~, internal and regulatory ~~own funds~~capital and liquidity ~~(~~reserves~~). This information shall relate in particular to the state of internal control.~~ .

~~49.~~62. Once a year, the authorised management shall confirm compliance with this Circular to the CSSF by way of a single written sentence followed by the signatures of all the members of the authorised management. Where, due to non-compliance, the authorised management is not able to confirm full compliance with the Circular, the aforementioned statement takes the form of a reservation which outlines the non-~~compliance~~compliant items by providing explanations on their raison d'être.

~~For credit institutions, the information to be provided to the CSSF pursuant to the first paragraph shall be submitted to the CSSF together with the annual accounts to be published.~~

~~50.~~63. Where the authorised management becomes aware that the central administration and internal governance arrangements no longer enable a sound and prudent ~~business~~ management of the activities or that the ~~risks~~ incurred risks are or will no longer be properly borne by the institution's ability to manage these risks, by the internal and regulatory ~~or internal own funds or~~capital and liquidity reserves, it shall inform the Board of Directors and the CSSF by providing them, without delay, with any necessary information to assess the situation ~~(cf. also point 22).~~.

~~[13] Cf. point 26 of Circular CSSF 07/301.~~

~~51.~~64. Notwithstanding the ~~overall~~joint responsibility of the members of the authorised management ~~(cf. point 72),~~ it shall designate at least one of its members ~~to~~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. ~~S/he~~This member shall be in charge, in particular, ~~in charge~~ of ~~developing~~drawing up the organisation chart and the task description ~~(cf. point 68)~~ which s/he submits, prior to their implementation, to the authorised management for approval. S/he then shall ensure their proper ~~implementation.~~application. The member in question shall also be in charge of the ~~provision~~production and publication of accounting information intended for third parties and the transmission of periodic information to the CSSF. Thus, s/he shall ensure that the form and content of this information comply with the legal rules and ~~the rules~~instructions of the CSSF in this field.

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

~~52.~~65. The institutions shall ~~provide~~inform the CSSF ~~with information on the persons referred to in point 105. The authorised management shall report to the CSSF in writing and as soon as possible, on~~ of the appointments and ~~revocations of these persons by giving~~ removals of the members of the authorised management, in accordance with the ~~grounds~~provisions of this Circular and the Prudential Procedure, stating moreover the reasons for ~~revocation~~the removal.

Section 4.2.2. Qualification of the authorised management

~~53.~~66. The members of the authorised management shall, both individually and collectively, ~~should~~ have the necessary professional ~~competences (expertise, understanding~~qualifications (appropriate knowledge, skills and experience), the professional ~~standing~~repute and personal qualities to manage the institution and ~~effectively~~ determine the business direction effectively. The personal qualities shall be those which enable them to ~~properly~~effectively perform their authorised manager's mandate with the required commitment, availability, objectivity, critical thinking and independence of mind.

~~**Section 4.2.3. Specific (risk, capital and liquidity) policies**~~

~~15. The risk policy which implements the risk strategy of the board of directors shall include:~~

- ~~the institution's risk tolerance determination;~~

- the definition of a complete and consistent internal limit system 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 tolerance. 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 pursuant to point 11;
- the measures to be implemented in order to ensure that risk taking and management comply with the set policies and limits. These measures shall include in particular the existence of a risk control function and management arrangements for limit breaches, including corrective measures of 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).

Pursuant to the provisions of Part III, Chapter 2, of this circular, the risk policy shall take due account of risk concentrations.

16. The capital and liquidity policy implementing the strategy of the board of directors in respect of regulatory and internal own funds and liquidity shall include, in particular:

- the definition of internal standards in relation to the management, scope and quality of the regulatory and internal own funds and liquidity reserves. These internal standards shall 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 own funds and liquidity reserves, in particular in relation to own funds and internal capital 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 own funds and liquidity reserves;
- the measures taken in order to effectively manage stress situations (regulatory or internal capital inadequacy or liquidity crisis);
- 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.

Chapter 5. Administrative, accounting and IT organisation

Sub-chapter 5.1. Organisation chart and human resources

~~54.~~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. ~~These decision-making and implementation tasks, including the initiation, recording, follow-up and monitoring of the operations, and the internal control tasks are carried out on the basis of an organisation chart of the functions and task description adopted by the authorised management in writing. The organisation chart and task description are~~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.

~~55.~~68. The ~~organisation chart shall show for~~ structure of the different functions (business, support and control) ~~functions as well as for~~and of the different business units ~~(services, departments or positions) their structure and~~ must be presented in the organisation chart, along with the reporting and ~~business~~functional lines ~~between them~~with each other and with the authorised management and the Board of Directors.

~~56.~~69. The task description to be filled in by the operating staff shall explain the function, powers and responsibility of each officer.

~~57.~~70. ~~Without prejudice to point 72,~~ 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 ~~that they are~~making them incompatible for the same person. The goal pursued ~~is~~shall be to avoid conflicts of interest and to prevent, through ~~a peer review~~reciprocal control environment, a person from making mistakes and irregularities which would not be identified.

~~58.~~71. Pursuant to ~~Articles 7 (2) and~~Article 19(2) of the LFS, the authorised management shall be jointly liable for the management of the institution. The principle of segregation of duties ~~cannot~~shall not derogate from this joint liability. ~~Moreover,~~ 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. ~~In this context, the CSSF recommends to~~The institution must organise this ~~segregation~~allocation so as to avoid conflicts of interest. Thus, ~~it is advisable not to assign the~~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 ~~to the same member of the authorised management.~~. Similarly, the authorised manager who himself/herself serves as Chief Compliance Officer and/or Chief Compliance Officer pursuant to point ~~141~~134 and/or point 148 of this part, cannot, at the same time, be in charge of the internal audit function~~.~~ (cf. incompatibility of functions in the box below). Where, due to the small size of the institution, several duties and responsibilities have to be assigned to the same person, this grouping ~~shall~~must be organised so that it does not prejudice the objective pursued by the segregation of duties.

Incompatibility of functions:

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

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

60.73. Each employee shall annually staff member must take at least tentwo consecutive calendar weeks of personal days off.leave annually. It must be assured that the employeeeach staff member is actually absent during that leave and that his/her substitute actually takes charge of the work of the absent person.

Sub-chapter 5.2. AdministrativeProcedures and technical infrastructure

17. The institution shall have support functions, necessary and sufficient material and technical resources to execute its activities. In this respect, the principles laid down in Sections 5.2.1 to 5.2.5 shall apply.

Section 5.2.1. Administrative infrastructure of the business functions

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

Section 5.2.2. Financial and accounting function

61.1. The institution shall have a financial and accounting department whose mission is to assume the accounting 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 shall ensure that other departments intervene in full compliance with the chart of accounts and the instructions relating thereto. The central department shall remain responsible for the preparation of the annual accounts and the preparation of the information to be provided to the CSSF.

19. The financial and accounting function shall operate based on written procedures which aim to:

- identify and record all transactions undertaken by the institution;
- explain 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;
- prepare the accounts by applying all the valuation and accounting rules laid down by the relevant accounting laws and regulations;
- verify the reliability and relevance of the market prices and fair values used while preparing the accounts and reporting to the CSSF;
- issue periodic information including, first, the legal and regulatory reporting, and to provide the CSSF with it, and to ensure its reliability, particularly in terms of solvency, liquidity and large exposures;
- keep all accounting documents in accordance with the applicable legal provisions;
- draw up, where appropriate, accounts according to the accounting scheme applicable in the home country of the shareholder in order to prepare consolidated accounts;
- undertake the reconciliation of accounts and accounting entries;
- provide accurate, complete, relevant, understandable management information available without delay which shall enable the authorised management to closely monitor the developments in the financial situation of the institution and its compliance with budget data. This information shall be used as management control tool and will be more effective if it is based on analytical accounting;
- ensure the reliability of the financial reporting.

20. 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.

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

22. In connection with opening 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 also specify the conditions for opening, closing and operating these accounts.

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

~~The opening and closing of~~ internal ~~accounts in the accounting records shall be validated by the financial and accounting department. In case of opening accounts, this validation shall 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 justification procedure.~~ documentation

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

~~62.1.~~ ~~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 both within the departments which are at the origin of these entries and within the financial and accounting department.~~

~~23. The entire accounting organisation and procedures shall be described in an accounting procedure manual.~~

~~While defining and implementing these procedures,~~ The institutions shall ~~ensure compliance with the principle of integrity (point 12) in order to avoid in particular that the accounting system is used for fraudulent purposes.~~

~~Section 5.2.3. IT function~~

~~24. Institutions shall organise their IT function so as to have control over it and to ensure robustness, effectiveness, consistency and integrity pursuant to point 12.~~

~~These requirements are best fulfilled when the IT function of the institution is performed by its own IT department which is organised and framed by internal control arrangements established by the authorised management. Generally, the institution shall have, in premises at its disposal in Luxembourg, its own computers and adequate and duly documented IT programmes and hire competent staff to manage its IT system.~~

~~The institution shall be in a position to ensure normal operations in case of an IT system outage and shall have a backup solution in line with a business continuity and recovery plan.~~

~~The institutions shall have a monitoring process in place in order to be quickly informed of the emergence of new security vulnerabilities, as well as a procedure to manage patches allowing the correction of these vulnerabilities, within a short period of time, if they can significantly impact their IT systems. Internal audit shall include the review of the monitoring process and the management of patches in its multi-annual audit plan; it shall notably state any failures in the launch of production of a patch while this patch is widely known and shall~~ document ~~such failure in an audit finding.~~

~~25. Institutions shall appoint a staff member who is responsible for the IT function. This person is referred to as the IT Officer. In smaller institutions, this responsibility may be assumed by a member of the authorised management who may rely on external expert advice.~~

~~Moreover, institutions shall appoint a staff member who is responsible for the security of information systems. In smaller institutions, this responsibility may be assumed by a member of the authorised management who may rely on~~

external expert advice. This person is referred to as the Information Security Officer (ISO) or, in French, the "Responsable de la Sécurité des Systèmes d'Informations". The ISO shall be the person in charge of the organisation and management of the information security, i.e. the protection of the information. S/he shall be independent from the operational functions and, depending on his/her position and the size of the undertaking, released from the operational implementation of security actions. An escalation mechanism shall enable her/him to report any exceptional problem to the highest level of the hierarchy, including the board of directors. His/her key missions are the management of the analysis of the risks related to information, the definition of the required organisational, technical, legal and human resources, the monitoring of their implementation and effectiveness as well as the development of the action plan(s) aimed to improve the risk coverage.

In smaller institutions, a single member of the authorised management may take on the duties as IT Officer and ISO. S/he may rely on external expert advice.

26. Institutions which rely on third parties as regards the IT function shall comply, in particular, with the conditions laid down in Section 7.4.2.

Section 5.2.4. Internal communication and whistleblower arrangements

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

28. The management information system shall ensure that the management information is, in normal circumstances and in times of stress, transmitted in a clear and comprehensive manner and without delay to all members of the board of directors, the authorised management and staff of the institution by taking into account their information needs, responsibilities within the institution and the objective to ensure sound and prudent business management.

29. The institutions shall maintain internal whistleblower arrangements which enable the entire staff of the institution to draw attention to serious and legitimate concerns about internal governance. These arrangements shall respect the confidentiality of the persons who raise such concerns and provide for the possibility to raise these concerns outside the established reporting lines as well as with the board of directors. The warnings given in good faith shall not result in any liability of any sort for the persons who issued them.

Section 5.2.5. Crisis management arrangements

63.1. 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.

30. The crisis management arrangements shall ensure that, in times of stress, the credit institutions provide the public with the information referred to in the EBA guidelines published on 26 April 2010 ("Principles for disclosures in times of stress (Lessons learnt from the financial crisis)"). This point shall not apply to investment firms.

~~31. The crisis management arrangements shall be tested and updated in a regular basis in order to ensure and maintain its effectiveness.~~

~~Sub-chapter 5.3. Internal documentation~~

~~64.~~74. ~~The institutions shall document in writing~~ 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 ~~in particular~~ a clear ~~and~~, comprehensive ~~procedure manual which is easily~~, detailed and accessible ~~to~~manual of procedures, whose procedures shall be known by the ~~institution's~~entire staff concerned and which is updated on an ongoing basis.

~~65.~~75. The description of the procedures ~~for~~to ensure the proper execution of activities ~~(transactions) concerns~~shall concern the following points:

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

~~As the purpose is to ensure that the transactions are properly executed, the procedures' content should be clear, updated, comprehensive and made known to all relevant employees.~~

~~66.~~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 ~~shall~~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.

~~By way of illustration 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 evolution of the debtor's financial situation.~~

~~67.~~77. The files, working papers and control reports of the internal control functions, experts and subcontractors referred to in Sub-chapter 6.2 of this part as well as the long ~~-~~form reports drawn up by the ~~*réviseurs*~~*réviseur d'entreprises agréé* shall be kept ~~during five years~~ in the Luxembourg institution during at least five years, without prejudice to other applicable laws, in order to enable the institution to ~~track~~retrace the controls carried out, the identified problems, shortcomings or irregularities ~~identified~~ as well as the recommendations and conclusions. The CSSF as well as the *réviseur d'entreprises agréé* ~~shall~~must always be able to access these documents.

~~68.~~78. All transaction orders initiated by the institution and all correspondence with the customers or their proxies shall be issued by the institution; all correspondence shall be addressed thereto. In the case where the institution has a branch abroad, the latter is the contact point for its own customers.

Sub-chapter 5.3. Administrative and technical infrastructure

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

Section 5.3.1. Administrative infrastructure of the business functions

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

Section 5.3.2. Financial and accounting function

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

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

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 CSSF;
- the production and transmission of periodic information, including, primarily, the legal and regulatory reporting, to the CSSF, ensuring the information is reliable, particularly in terms of solvency, liquidity, non-performing loan exposures, restructured credits and large exposures;
- the record-keeping of all accounting documents in accordance with the applicable legal provisions;
- the drawing-up of, where appropriate, accounts according to the accounting scheme applicable in the home country of the shareholder in order to prepare consolidated accounts;
- the completion of reconciliation of accounts and accounting entries;
- the production of accurate, complete, relevant, understandable management information available without delay which shall enable the authorised management to take informed decisions and to closely monitor the developments in the financial situation of the institution and its compliance with budget data. This information shall be used as a management control tool and will be more effective if it is based on analytical accounting;
- the guarantee that the financial reporting is reliable.

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.

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.

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 Board of Directors and authorised management, directly or by way of delegation, are communicated in a clear and comprehensive manner to all staff members of the institution, considering their information needs and their responsibilities within the institution. The internal communication arrangements shall enable staff to have easy and constant access to this information.

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

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

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).

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

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

Commission de Surveillance du Secteur Financier

Chapter 6. Internal control

~~69.~~98. The internal control ~~is~~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 ~~economically and~~ 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 ~~applications~~requests and requirements of the CSSF are met~~.~~[14].

~~32. A suitable~~The internal control ~~environment requires~~arrangements of an institution must be adapted to its organisation and to the ~~implementation of the following controls:~~

- ~~day-to-day controls carried out by the operating staff as provided for in Section 6.1.1;~~
- ~~ongoing critical controls carried out by the staff in charge~~nature, scale and complexity of ~~the administrative processing of transactions as specified in Section 6.1.2;~~

~~70.~~99. ~~controls carried out by the members of the authorised management on the~~ its activities ~~or functions which fall under their direct responsibility as specified in Section 6.1.3;~~and relating risks and comply with the principles of the "three lines of defence" model.

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

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

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.~~controls~~

[14] *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, ~~in particular~~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.*

~~carried out by the internal control functions as defined in Sub-chapter 6.2.~~

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

Sub-chapter 6.1. Operational controls

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

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

~~71.~~100. 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 ~~employee~~staff member.

Section 6.1.2. Ongoing critical controls

~~72.~~101. This category of controls shall include inter alia:

- hierarchical control;
- validation (for example dual signature, codes of access to specific features) ~~regarding~~associated with the monitoring of compliance with the authorisation procedure and procedure for delegating powers adopted by the authorised management ~~(in particular as regards credit);~~;

~~• peer reviews;~~

- ~~establishment~~reciprocal controls;
- regular statement of the existence ~~of~~and the value of the assets and liabilities, ~~on a regular basis,~~ 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 ~~persons in charge~~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 ~~concluded~~, 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 ~~shall be~~is guaranteed only if the principle of segregation of duties is complied with.

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

~~73.~~102. 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 ~~are~~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~~the members of the authorised management are inter alia:

- the risks associated with the activities and functions for which they are directly responsible;
- the compliance with the laws and standards applicable to the institution, with a particular emphasis on prudential standards on solvency, liquidity and regulations on large exposures;
- the compliance with the policies and procedures established by the authorised management ~~pursuant to point 18~~;
- 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;
- ~~evolution~~the development of the overall profitability of an activity.

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

Commission de Surveillance du Secteur Financier

Sub-chapter 6.2. Internal control functions

~~74.~~103. The policies implemented with respect to risk control, compliance and internal audit ~~pursuant to point 18~~ 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 ~~(cf. point 9).~~. Moreover, these policies ~~which~~shall describe the fields of intervention directly related to each internal control function ~~shall~~, clearly define the responsibilities for the common fields of intervention ~~and~~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.

~~33. Each internal control function shall be under the responsibility of a separate head of the function who shall be appointed and revoked in accordance with an internal written procedure. Where, in application of the principle of proportionality, a single member of the authorised management performs compliance and risk control functions, this person shall combine, as an exception to the foregoing, the positions of head of the compliance function and risk control function (cf. also point 72). The appointments and revocations of the persons in charge of the internal control functions shall be approved by the board of directors and reported in writing to the CSSF in compliance with the prudential authorisation procedure of key function holders as published by the CSSF on its website.~~

~~The persons in charge of the three internal control functions shall be responsible vis-à-vis the authorised management and ultimately vis-à-vis the board of directors for the performance of their mandate. In this respect, these persons shall be able to contact and inform, directly and on their own initiative, the chairman of the board of directors or, where appropriate, the members of the audit committee.~~

~~The persons in charge of the internal control functions are referred to as Chief Risk Officer for the risk control function, Chief Compliance Officer for the compliance function and Chief Internal Auditor for the internal audit function.~~

Section 6.2.1. General responsibilities of the internal control functions

~~75.~~104. The main purpose of the internal control functions ~~is~~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 ~~suitability as regards~~adequacy with respect to the organisational and operational structure, the strategies, the activities and the risks of the institution as well as ~~as regards~~with respect to the applicable legal and regulatory requirements, and to report directly to the authorised management as well as to the Board of Directors ~~pursuant to point 116.~~and, where appropriate, to the specialised committees. They shall provide the authorised management and the Board of Directors, and, where appropriate, the specialised committees with the opinions and advice they deem ~~necessary in order to improve the central administration and internal governance arrangements of the institution.~~ useful or which are requested by these bodies or committees.

~~76.~~105. ~~The internal control functions shall respond as soon as possible to the requests for advice and opinions from the authorised management and the board of directors or, where appropriate, the specialised committees. If~~Where they consider that the effective, sound or prudent business management is ~~challenged~~compromised, the ~~persons responsible for~~heads of the internal control functions~~,~~ shall promptly inform, on their own initiative, the authorised management and the Board of Directors or, where appropriate, the specialised committees ~~in accordance with the applicable internal procedures~~.

~~77.~~106. 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 ~~and boards of directors~~ as well as to the authorised management and ~~board of directors of~~to the ~~institution pursuant to point 116~~Board of Directors of the group head.

Section 6.2.2. Characteristics of the internal control functions

~~78.~~107. The internal control functions shall be permanent and independent functions each with sufficient authority. The ~~persons in charge~~heads of these functions shall have direct access right to the Board of Directors or its ~~chairman~~chairperson or, where appropriate, ~~the chairmen of~~to the specialised committees ~~which are part of it~~, to the *réviseur d'entreprises agréé* of the institution as well as to the CSSF.

The independence of the internal control functions is incompatible ~~with the situation in which~~where:

- the staff of the internal control functions are in charge of tasks they are called upon to control ~~or tasks which are not related to their respective control area~~;

~~• the internal control functions are, from an organisational point of view, included in the business units they control or report hierarchically to them and~~

- 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 authority,~~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 ~~shall~~are called upon to control.

~~79.~~108. The authority which the internal control functions must have, requires that these functions ~~should~~ 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 ~~of the institution~~ they control) ~~deemed~~they deem necessary to fulfil their missions.

~~80.~~109. ~~The staff of~~ The internal control functions or third parties ~~(cf. point 118)~~ acting on behalf of these functions ~~shall~~must be objective ~~in~~when carrying out their work.

In order to ensure objectivity, the ~~persons in charge~~heads of the internal control functions shall ~~exercise~~be independent ~~thinking and judgement~~minded: they ~~should~~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.

~~Objectivity also requires that conflicts of interest are avoided.~~

~~81.~~110. ~~In order to ensure the effectiveness~~ The members of the internal control functions~~, its members shall~~ must, individually and collectively, possess high professional knowledge, skills and experience in the field of ~~banking and~~ financial activities ~~and~~, especially in their field of responsibility with respect to applicable standards. ~~This competence shall be assessed by taking into account both~~In accordance with the principle of proportionality, the ~~nature of~~ required skill level shall increase with the ~~missions~~organisation of the ~~associates and the complexity and diversity of the activities carried out by the~~ institution ~~in order to enable thorough coverage~~ and the nature, scale and complexity of the activities and risks. ~~This~~The individual ~~competence shall~~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 ~~persons in charge~~heads of the internal control functions, who take on such a position for the first time, shall have the necessary theoretical knowledge ~~that enables them to effectively perform this function~~.

~~82.~~111. 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 ~~budgets, pursuant to~~budget, in keeping with the principle of proportionality ~~(point 4).~~. The budget ~~shall~~must be sufficiently flexible to reflect an adaptation of the missions of the internal control functions in response to changes ~~of~~in the institution's ~~risk profile. These provisions are compatible with the outsourcing of~~organisation, the activities and risks or upon the ~~internal audit function and the use of internal control functions to external experts pursuant to points 117 and 118.~~ occurrence of specific events.

~~83.~~112. The scope of intervention of the internal control ~~framework~~functions shall cover the whole institution within the limits of ~~its~~their respective competences. It shall include ~~the~~ non-standard and potentially non-transparent activities ~~referred to in Section 7.1.1~~.

~~84.~~113. Each institution shall take the necessary measures to ensure that the members of the internal control functions perform their functions with integrity and discretion.

Section 6.2.3. Execution of the internal control ~~functions'~~ functions' work

~~85.~~114. The internal control functions shall document the work carried out in accordance with the assigned responsibilities, in particular in order to allow ~~tracking~~retracing the interventions as well as the conclusions reached.

~~86.~~115. The internal control functions shall report, in writing, on a regular basis and, if necessary, on an ad hoc basis, to the authorised management and the Board of Directors or, where appropriate, to the specialised committees. These reports shall concern the follow-up ~~of~~to the recommendations, problems, shortcomings and irregularities ~~identified~~found in the past as well as the new identified problems, shortcomings and irregularities ~~identified~~. Each report shall specify the risks related thereto as well as their ~~seriousness (measurement of~~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~~ of~~, the ~~main recommendations on~~ (existing or emerging) problems, ~~significant~~the major shortcomings and irregularities found since the last report~~,~~ and the measures taken in this respect as well as the statement of the~~ significant~~ problems, shortcomings and irregularities identified in the last report but which have not yet been ~~the~~ subject ~~of~~to appropriate corrective measures.~~ The report shall also provide information on the activities linked to the other responsibilities of the control function, including those defined in Sections 6.2.5, 6.2.6 and 6.2.7.~~ Finally, the report shall indicate the state of their control area as a whole. As far as operation is concerned, the report shall~~ mention~~, in particular, comment on the adequacy of the internal human and technical resources, and the nature and level of reliance on external ~~experts pursuant to point 118~~human and technical resources as well as on any problems which may have occurred in this context. This report shall be submitted for approval to the Board of Directors ~~and, where appropriate,~~or the competent specialised committees ~~for approval~~to ensure its follow-up and that the Board of Directors is informed; it ~~is~~shall be submitted for information to the authorised management~~ for information~~.

~~Pursuant to point 107,~~ In case of serious problems, shortcomings and irregularities, the ~~persons in charge~~heads of the internal control functions shall immediately inform the authorised management, the ~~chairman~~chairperson of the Board of Directors and, where appropriate, the ~~chairmen~~chairpersons of the specialised committees~~ thereof~~. In such cases, the ~~CSSF recommends that the persons in charge~~heads of the internal control functions ~~are~~may request to be heard by the specialised committees in a private meeting.

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

Section 6.2.4. Organisation of the internal control functions

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

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

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

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

The operational tasks of the internal audit function ~~can~~may be outsourced by ~~smaller~~small institutions ~~whose risk profile is~~ with a low and non-complex~~, subject to the conditions laid down in point 118 and Sub-section 6.2.7.4. This kind of~~ risk profile. Such outsourcing is not, in principle, ~~not~~ acceptable for institutions with agencies, branches or subsidiaries.

The Board of Directors of the institution shall remain ultimately responsible for outsourcing the internal audit operational tasks. External providers entrusted with the outsourced internal audit operational tasks shall depend on and report directly to the member of the authorised management in charge of internal audit. They shall also have direct access to the Board of Directors or, where appropriate, the chairperson of the audit committee.

~~87.~~119. The provisions of the preceding point ~~112 do~~shall not exclude the possibility for the internal control functions to use the expertise and human or technical ~~resources~~means of third parties (belonging or not to the same group as the institution) for certain aspects. This use ~~is~~shall be governed by an internal procedure which ~~shall~~must allow, in particular, ~~enable~~ the authorised management and the Board of Directors to assess the dependencies and risks ~~for the institution arising from~~which a significant use of these ~~third parties.~~external resources might pose for the institution.

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

~~88.~~120. ~~The~~Any use of ~~an~~ external ~~expert shall~~resources must be based on a written mandate. ~~The expert~~These third parties shall carry out ~~his/her~~their work in ~~compliance~~accordance with the regulatory and internal provisions ~~(including the internal audit and compliance charters) which are~~ applicable to the internal control function and the area of control in question. ~~The expert shall~~ They must be placed under the ~~dependence~~authority of the ~~person in charge~~head of the internal control function covering the controlled area. This ~~person supervises~~head shall supervise the ~~experts'~~ work~~.~~ of these third parties.

121. ~~Pursuant to point 3, the internal control functions of an institution shall also be put in place~~Where the institution can demonstrate, in accordance with the principle of proportionality, that there is no justification for setting up a distinct risk control function and compliance function or for appointing two heads of these functions full time, the institution may either set up a combined function or a position with combined responsibility or entrust two different persons with these functions on a part-time basis, subject to prior approval of the CSSF.

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

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

122. The institution wishing, in accordance with the principle of proportionality, to outsource the operational tasks of the internal audit function must submit a prior request to the CSSF which shall include:

- the analysis and its conclusions justifying the outsourcing of the operational tasks of the internal audit function;
- the decision of the Board of Directors approving the analysis and its conclusions and, where appropriate, the opinion of the audit committee;

- a 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; and
- the person in charge of this outsourcing within the institution.

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

~~89.~~123. The internal control functions of an institution must also be set up at ~~the~~group level ~~of~~, in the ~~group,~~ legal entities and in the branches composing ~~it~~the group. These constituent parts ~~shall~~must each have their own internal control functions, ~~taking into account~~considering the principle of proportionality ~~as indicated in point 4.~~ .

~~90.~~124. Within the branches ~~of the institution~~, the internal control functions shall depend, from a hierarchical and functional point of view, on the control functions of the ~~group head~~ legal entities to which they belong and ~~to which they~~ report.

~~As regards~~Within the subsidiaries, the internal control functions shall depend, from a functional point of view, on the control functions of the group head ~~to which they belong.~~ . The reports drawn up in accordance with the provisions of this Circular shall be submitted ~~both~~not only to the local authorised management and ~~supervisory bodies~~Board of Directors but also, in summarised form, to the internal control functions of the ~~parent~~group head institution which ~~analyses~~shall analyse them and ~~reports~~report the ~~points~~items to be noted in accordance with point ~~116~~115.

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

Where the institution is a not ~~the~~ parent undertaking ~~within the meaning of point 3, the institution~~, 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~~115.

~~In accordance with point 4, the institution can relinquish the option of putting in place own internal control functions within legal entities or branches of the~~

group. In this case, the institution shall ensure that its internal control functions carry out controls, including on-site inspections on these entities on a regular basis.

91.125. The principles of this Circular doshall not exclude that, for Luxembourg institutions which are, whether or not branchthey are branches or subsidiarysubsidiaries 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.

Comments:

1. Reference is made to points 9, 17, 21, 33, 45 to 51, 57, 104 to 121, 147Scope and 179 also relating to specific responsibilities of the risk control function.

2. The term "risk control function" is borrowed from the "EBA Guidelines on Internal Governance (GL 44)". This terminology is not aimed to reduce this function to a mere ex post risk limit "control" as referred to in the second sentence of point 124. The risk control function shall more broadly take on risk analysis and follow-up tasks in accordance with point 123.

3. The risk control function shall submit a copy of its summary annual report to the CSSF (points 116 and 210). Pursuant to point 116, this report includes the current state of risks and thus possibly duplicates the ICAAP report (point 61) drawn up by the authorised management for the board of directors. The risk of duplication exists, especially considering that, in general, the risk control function is associated with the drafting of the ICAAP report. For the sake of avoiding any undue duplication between the ICAAP report and summary report of the risk control function, it is sufficient, for the risk assessment in line with the ICAAP, that the risk control function makes reference to the ICAAP report in its summary report, insofar as it shares the risk descriptions and analyses included therein. Where it does so, the risk control function shall nevertheless issue, in its summary report, its own conclusions drawn from the aforementioned descriptions and analyses. The summary report shall then deal exclusively with the other areas referred to in point 116. However, when the risk control function does not share the aforementioned descriptions and analyses, it shall explicitly mention it in its summary report in which it includes its own assessments.

4. Another possible duplication field exists in respect of the segregation of duties between the compliance function in charge of the risk compliance (point 131) and the risk control function in charge of "all risks" (point 123). The institutions shall ensure that these tasks are internally assigned in an effective and efficient way.

34. The risk control function is entrusted to a dedicated department composed of one or several persons.

35. The risk control function is in charge of the anticipation, identification, measurement, monitoring, control and reporting of all the risks to which the institution is or may be exposed. Thus, it shall assist the authorised management in limiting the risks. It shall ensure that the risks are properly managed.

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

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

~~92.~~127. The scope of intervention of the risk control function shall ~~also include~~cover the whole institution, including the risks associated with the complexity of the institution's legal structure ~~of the institution~~ and the relationships of the institution with related parties.

~~Sub-section 6.2.5.1. Specific responsibilities and scope of the risk control function~~

~~93.~~128. The risk control function shall ensure that the ~~regulatory and~~ 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~~ and the proper application~~, propose appropriate remedial measures in case of breach, ensure compliance with the escalation procedure ~~provided for~~ in case of significant breach and ~~shall~~ ensure that the breaches are remedied as soon as possible.

~~94.~~129. The head of the risk control function shall ensure that the authorised management and the Board of Directors receive ~~a~~an independent, comprehensive, objective and relevant overview of the risks to which the institution is or may be exposed. This overview shall include, in particular, an assessment of the ~~adequacy~~correlation between these risks and the own funds and liquidity ~~(~~reserves~~)~~ and the ~~institution's~~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 ~~as regards~~of the ~~adequacy~~correlation between the risks incurred and the ~~strategies laid down~~risk appetite defined by the Board of Directors. The frequency of this communication shall be adapted to the institution's characteristics and needs, in ~~particular regarding the risk tolerance.~~ view of its business model, the risks incurred and its organisation.

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

~~95.~~130. The risk control function shall ensure that the terminology, ~~methods~~methodology and technical resources used for the risk anticipation, identification, measurement, reporting, management and ~~monitoring~~control are consistent and effective.

~~96.~~131. The risk control function shall ensure that the ~~qualitative and quantitative~~ risk assessment is based on conservative assumptions and on a range of relevant scenarios, in particular regarding dependencies between risks. ~~The~~ Quantitative assessments ~~are to~~shall be validated by qualitative ~~(~~assessment methods and expert~~)~~ judgements based on structured and documented analyses.

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

~~97.~~132. The risk control function shall strive to anticipate and recognise the risks arising in a changing environment. In this respect, it shall also monitor the implementation of the changes in the activities ("New Product Approval Process") in order to guarantee that the associated risks ~~relating thereto~~ remain ~~controlled.~~ under control.

Sub-section 6.2.5.2. Organisation of the risk control function

~~36. Where, pursuant to the principle of proportionality (point 4), the creation of a full-time position of Chief Risk Officer is not necessary, a person may be entrusted with this position on a part-time basis.~~

~~It is appropriate to ensure that the other tasks performed by this employee remain compatible with the responsibilities incumbent upon him/her pursuant to the provisions of this circular.~~

~~The institution which is not willing to create a full-time position of Chief Risk Officer shall inform the CSSF by stating the grounds of its decision.~~

133. ~~It is acceptable for the~~ 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.

~~98.~~134. Subject to specific authorisation by the CSSF, the member of the authorised management designated as ~~being~~ directly in charge of the risk control function ~~to assume~~ may take up the position of Chief Risk Officer himself/herself ~~the position of Chief Risk Officer~~.

Within the significant institutions, the head of the ~~Section 6.2.6. Compliance function~~

> ~~***Comments:***~~
>
> ~~*1. Reference is made to points 9, 17, 21, 33, 44, 55, 57, 104 to 121, 147 and 179 also relating to the compliance function.*~~
>
> ~~*2. There might be a duplication in respect of the segregation of duties between the compliance function in charge of the compliance risks (point 131) and the* risk control function *in charge of "all risks" (point 123). The institutions shall ensure that these tasks are internally assigned in an effective and efficient way.*~~

~~37. The compliance function is entrusted to a dedicated department composed of one or several persons.~~

~~99.~~135. ~~The aim of the compliance function is to anticipate, identify and assess the compliance risks of an institution as well as to assist the~~ shall be a member of the authorised management ~~in limiting these risks. These risks may include a variety of risks such as the reputational risk, legal risk, risk of dispute, risk of sanctions, as well as some operational~~ who is independent and individually responsible for the risk ~~aspects, in connection with all activities~~ 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.

~~This task is to be performed on an ongoing basis and without delay.~~

The ~~institutions which provide investment services within the meaning~~ head of the ~~LFS shall implement a compliance~~ risk control function ~~which complies with~~ must be able to challenge the decisions of the ~~ESMA guidelines of 6 July 2012 (Guidelines on certain aspects of the MiFID compliance function requirements (ESMA/2012/388)).~~

~~**Specification:**~~

~~100.~~136. ~~This circular includes "general guidelines" included in the document ESMA/2012/388 and applies them to all activities of~~ 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 ~~provision~~escalation process of ~~investment services. Where they implement these requirements in relation to the investment services within the meaning~~the Board of ~~the LFS, the institutions shall take into account the "supporting guidelines" set out in the document ESMA/2012/388~~Directors.

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

Section 6.2.6. Compliance function

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

Sub-section 6.2.6.1. Compliance charter

~~101.~~137. The ~~terms of operation~~operational arrangements of the compliance function in terms of objectives, responsibilities and powers ~~are~~shall be laid down in a compliance charter drawn up by the compliance function and approved by the authorised management and ultimately by the Board of Directors.

~~102.~~138. The compliance charter ~~shall~~must at least:

- define the position of the compliance function in the organisation chart of the institution ~~by~~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 ~~inquiries on~~investigations about all activities of the institution, including those of its branches and subsidiaries in Luxembourg and abroad, and the right to access ~~to~~ 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;
- ~~establish~~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 ~~chairman~~chairperson of the Board of Directors or, where appropriate, the members of the audit committee or the compliance committee as well as the CSSF.

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

~~103.~~139. The compliance charter ~~shall~~must be updated as soon as possible in order to take into account the changes in the applicable standards affecting the institution. Any changes ~~shall~~must be approved by the authorised management, confirmed by the audit committee or, where appropriate, the compliance committee and ultimately approved by the Board of Directors. They ~~are~~shall be brought to the attention of all staff members.

Sub-section 6.2.6.2. Scope and specific responsibilities ~~and scope~~ 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.

~~104.~~141. For the ~~purpose~~purposes of reaching the objectives set, the responsibilities of the compliance function ~~shall~~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 ~~shall~~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 ~~shall~~ assess their significance and the possible consequences. The compliance risk classification so determined ~~shall~~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 ~~the~~ transactions and the network of ~~the~~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 ~~its~~their day-to-day tasks. These rules ~~shall~~must be ~~properly~~appropriately reflected in the instructions, procedures and internal controls ~~in~~of areas directly ~~related to compliance. In drawing up these rules,~~under the compliance function and shall take into account~~, as far as necessary for~~ the ~~institution in question, the~~institution's code of conduct ~~laid down in the internal governance arrangements.~~and corporate values;
- The areas falling directly ~~related to~~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 ~~integrity of the financial instruments markets~~frauds, the protection of the customers' ~~and investors'~~ interests~~, the~~ and data ~~protection~~ and ~~observance of professional secrecy, the avoidance~~ the prevention and management of conflicts of interest~~, the prevention~~. 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 ~~use of~~ compliance function, a copy of which shall be submitted to the ~~financial sector by third parties to circumvent their regulatory obligations and~~ CSSF, shall cover the ~~management of~~field of anti-money laundering and counter terrorist financing in a dedicated chapter laying down the ~~compliance risk related to cross-border~~ activities~~. In~~ and events relating to this area, i.e. the ~~more general context of compliance with the code of conduct, the compliance function has also to cover the fields of ethics and professional conduct~~main recommendations issued, major (existing or ~~even frauds. This list is not exhaustive.~~ 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. ~~However, insofar as some areas, resulting in practice in compliance risks, may also be linked to other functions such as the risk control function, finance function or legal function, and for the sake of avoiding any duplication of the compliance controls,~~ The areas other than those ~~referred to~~listed above may not be directly covered by the compliance function. ~~In this case, it~~ The compliance risk is ~~understood that the compliance risk is~~then to be covered by the other internal control functions in accordance with a compliance policy clearly defining the ~~competences~~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 ~~its competence~~his/her scope of intervention, are well covered.

~~• The institution is in charge of deciding whether, in view of the particular characteristics of the activities performed, its compliance function includes monitoring compliance with the rules that are not directly related to banking and financial activities, strictly speaking, such as in particular the rules under labour law, social law, company law or environmental law.~~

~~105.~~142. The compliance function shall verify compliance with the compliance policy and procedures, on a regular basis, and ~~is~~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 ~~as well as~~and the verification of the procedures and instructions, the provisions of this Circular ~~do~~shall not prevent the compliance function from taking into account the internal audit work.

~~106.~~143. The compliance function shall centralise all information on the compliance problems (inter alia ~~infringements~~internal and external frauds, breaches of standards, non-compliance with procedures and limits or conflicts of interest) identified by the institution.

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

~~107.~~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.

~~108.~~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.

~~109.~~146. The Chief Compliance Officer ~~is~~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 ~~is~~shall also be in charge of the transmission of any information or ~~statement~~report to these authorities.

Sub-section 6.2.6.3. Organisation of the compliance function

~~38. Where, pursuant to~~The institutions shall create a permanent and independent compliance function, considering the principle of proportionality ~~(point 4), the creation of a full-time position of Chief Compliance Officer is not necessary, a person may be entrusted with this position on a part-time basis.~~

~~It is appropriate to ensure that the other tasks performed by this employee remain compatible with the responsibilities incumbent upon him/her pursuant to the provisions of this circular.~~

~~110.~~147. ~~The institution which does not want to create a full-time position of Chief Compliance Officer, shall obtain explicit permission from the CSSF. To this end, the authorised management and the chairman of the board of directors shall submit to the CSSF a written request providing the grounds as well as the necessary information to enable to assess that the correct~~ and the criteria governing its application ~~of the provisions of this circular and the proper performance of the compliance function remain assured~~as well as general considerations regarding the organisation of the internal control functions laid down in Section 6.2.4.

~~111.~~148. Subject to specific authorisation by the CSSF, the member of the authorised management designated as directly in charge of the compliance function ~~himself/herself~~ may take up the position of Chief Compliance Officer himself/herself.

Section 6.2.7. Internal audit function

> ~~**Comment:**~~
>
> ~~Reference is made to points 9, 17, 21, 33, 38 to 44, 55, 57 and 104 to 121 also relating to the internal audit function.~~

~~39. The internal audit function is entrusted with the internal audit department, composed of one or several persons.~~

~~40. The audit function shall constitute within the organisation of the institution an independent and permanent function of critical assessment of the adequacy and effectiveness of the central administration, internal governance and business and risk management as a whole in order to assist the board of directors and authorised management of the institution and to enable them to best control their activities and the risks related thereto and thus to protect its organisation and reputation.~~

Sub-section 6.2.7.1. Internal audit charter

~~112.~~149. The ~~terms of operation~~operational arrangements of the internal audit function in terms of objectives, responsibilities and powers ~~shall~~must be laid down ~~by~~in an internal audit charter drawn up by the internal audit function and approved by the authorised management, confirmed, where appropriate, by the audit committee, and ultimately approved by the Board of Directors.

The internal audit charter ~~shall~~must at least:

- define the position of the internal audit function in the organisation chart of the institution ~~by~~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 ~~to~~ authorise it to review all the activities and functions of the institution including those of ~~their~~its branches ~~abroad~~ and subsidiaries in Luxembourg and abroad as well as the outsourced activities and functions, to access all documents, ~~instruments~~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 ~~can~~may be drawn from the audit missions;
- define the relationships with the compliance and risk control functions;
- ~~establish~~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 ~~person in charge~~head of the internal audit function;
- establish the right for the Chief Internal Auditor to, directly and on his/her own initiative, contact the ~~chairman~~chairperson of the Board of Directors or, where appropriate, the members of the audit committee as well as the CSSF;
- specify ~~that the internal audit missions are performed in accordance with the~~ the recognised professional standards~~15~~ governing the functioning and work of the internal audit[16];
- 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 ~~is~~shall be brought to the attention of all staff members of the institution, including those who work in branches ~~abroad~~ and subsidiaries in Luxembourg and abroad.

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

~~15 Such as for example the International Professional Practices Framework (IPPF) of the Institute of Internal Auditors (IIA)~~

16 Such as, for example, the International Professional Practices Framework (IPPF) of the Institute of Internal Auditors (IIA).

~~113.~~150. ~~In addition to points 110 to 112,~~ The internal audit department ~~has~~shall have a sufficient number of staff and ~~has~~have the required skills as a whole to cover all activities of the institution. The internal auditors ~~shall~~must have sufficient knowledge of the audit techniques.

In order not to ~~challenge~~jeopardise their independence of judgement, the persons ~~responsible for~~from the internal audit cannot be in charge of the preparation ~~or~~and establishment of elements of the central administration and internal governance arrangements. This principle ~~does~~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 ~~(cf. in particular point 107).~~. Moreover, in order to avoid conflicts of interest, a rotation of the control tasks assigned to the various internal auditors ~~should~~shall be ensured, where possible, and it should be avoided that the auditors hired within the institution ~~control~~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

~~114.~~151. ~~In general,~~ The internal audit function shall ~~review~~examine and assess ~~whether the central administration~~, among others (non-exhaustive list[17]), the following in accordance with the organisation and ~~internal governance arrangements are adequate~~the nature, scale and ~~operate effectively. In this respect, the internal audit function shall assess *inter alia:*~~ complexity of the activities:

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

[17] *Principle 7 of the document "BCBS 223 The internal audit function in banks" contains a more comprehensive list of activities which may fall within the scope of the institutions' internal audit function.*

- accurate and complete registration of the transactions and the ~~provision~~production of accurate, complete, relevant and understandable financial and prudential information available without delay to the Board of Directors~~, specialised committees~~ and, where appropriate, the specialised committees, to the authorised management and the CSSF;
- implementation of the decisions taken by the authorised management and by the persons acting by delegation and under its responsibility;
- compliance with the policies and procedures, in particular those governing ~~the~~capital adequacy ~~of the regulatory~~ and internal ~~own funds and~~ liquidity ~~(~~reserves~~) in accordance with points 67, second and third indents, and 125~~;
- adequacy of the risk management;
- integrity of the processes ensuring the reliability of the methods and tools used by the institution, the assumptions and data used in the internal models, the qualitative tools for risk identification and assessment, as well as the risk mitigation measures taken;
- operation and effectiveness of the compliance and risk control functions ~~(Sections 6.2.5 and 6.2.6).~~ .

~~115.~~152. Where there is, within ~~an~~the institution, a separate department in charge of the control or supervision of a specific activity or function, the existence of such a department ~~does~~shall not discharge the internal audit department from its responsibility to ~~control~~audit this specific area. However, the internal audit department may take into account, in its work~~ the~~, assessments issued by this department on the area in question.

The internal audit ~~shall~~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.

~~116.~~153. ~~Further to points 119 and 120,~~ The establishment of a local internal audit function in the subsidiaries of the institution ~~does~~shall not discharge the internal audit of the group head from carrying out regular on-site inspections ~~on~~of these local internal audit functions.

~~41. The Chief Internal Auditor shall ensure that the department applies the international standards of the Institute of Internal Auditors or equal international standards in accordance with point 21 as well as the rules of conduct in accordance with point 55.~~

Sub-section 6.2.7.3. Execution of the internal audit work

~~117.~~154. All internal audit missions shall be planned and executed in accordance with an internal audit plan. The plan shall be established by the ~~person in charge~~head of the internal audit function for a period of several years (in general three years). Its purpose ~~is~~shall be to cover all activities and functions, ~~taking into account~~considering both the risks posed by an activity or function ~~of the institution~~ and the effectiveness of the organisation and internal control in place for this activity or function~~.~~ (risk-based approach). The plan ~~should~~shall consider the opinions issued by the Board of Directors ~~and~~or, where appropriate, the audit committee~~,~~ as well as the authorised management. The plan shall cover all matters of prudential interest (including the CSSF's ~~comments~~observations and requests) and shall also reflect the developments and innovations provided for as well as the risks which may arise therefrom.

~~118.~~155. The plan shall be discussed with the authorised management and ~~submitted to the authorised management and approved by it, confirmed~~, where appropriate, ~~by~~with the audit committee and ultimately approved by the Board of Directors. It shall be reviewed, on an annual basis, and adapted~~, where appropriate, in light of the~~ to developments and emergencies. ~~Any adaptation is to~~The plan shall be ~~formally approved~~reviewed by the authorised management and, where appropriate, by the audit committee~~.~~ before being approved by the Board of Directors. The approval implies that the authorised management provides the internal audit department with the means necessary to implement the internal audit plan.

In its summary report to the Board of Directors ~~in accordance with point 116~~, the internal audit shall indicate and state the reasons for the main changes brought to the audit plan as initially approved by the Board of Directors: cancelled missions, delayed missions as well as the missions whose scope ~~was~~has significantly changed.

~~119.~~156. The plan~~, which is adequately documented,~~ 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 ~~mission~~activity and risk.

The internal audit plan shall also provide for the adequate and sufficiently frequent coverage, within a multi-year planning period ~~of several years~~, of important or complex activities ~~which represent~~with a potential significant ~~potential~~ 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.

Commission de Surveillance du Secteur Financier

~~120.~~157. Where the internal audit department of the parent undertaking of the Luxembourg institution carries out on-site inspections ~~on~~of its subsidiary~~,~~ on a regular basis, it is recommended for reasons of effectiveness~~,~~ that, ~~insofar~~in so far as possible, the Luxembourg institution coordinates its internal audit plan with that of the parent undertaking.

~~121.~~158. The internal audit department shall regularly inform the authorised management and, where appropriate, the audit committee on the implementation of the internal audit plan.

~~122.~~159. Each internal audit mission shall be planned, executed and documented in compliance with the professional standards adopted by the internal audit function in its internal audit charter.

~~123.~~160. Each mission shall be the subject ~~to~~of a written report of the internal audit department~~, in general,~~ intended for the ~~supervised~~audited persons, the authorised management as well as - possibly in summarised form - for the Board of Directors (and, where appropriate, the audit committee~~) in accordance with point 116.~~). The reports shall also be made available to the *réviseur d'entreprises agréé* and the CSSF. These reports shall be ~~written~~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 ~~pursuant to point 116~~.

Sub-section 6.2.7.4. Organisation of the internal audit function

~~124.~~161. The ~~institution which, in line with point 117, decides to outsource the~~ institutions shall create a permanent and independent internal audit function, ~~shall submit a written request to~~ considering the principle of proportionality and the ~~CSSF. This request shall include the information necessary for~~criteria governing its ~~assessment, including, in particular,~~application as well as the considerations regarding the ~~name~~organisation of the ~~external expert (natural person) who will take on the~~ internal ~~audit function of the institution.~~ control functions laid down in Section 6.2.4.

~~The choice of the external expert, who carries out the internal audit work shall be approved by the board of directors, where appropriate, based on the opinion of the audit committee created in compliance with point 33. The selected expert shall be independent from the *réviseur d'entreprises agréé* and the *cabinet de révision agréé* of the institution as well as from the group to which these persons belong. It shall carry out the tasks in accordance with point 118 and *mutatis mutandis* the provisions of this circular. In this respect, it shall take over all duties and responsibilities incumbent upon the internal audit under this circular.~~

~~42. In case of use of an external expert for certain aspects in accordance with point 118, this expert shall carry out his/her~~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 ~~his/her~~their work and by drafting ~~the~~ reports for each mission. These reports ~~are to~~shall be drafted in French, German or English and ~~to be delivered to~~ submitted to the designated head of the ~~Chief Internal Auditor~~function, the authorised management, where appropriate, the audit committee and the Board of Directors ~~according to point 116.~~

~~125.~~162. ~~Pursuant to point 118, the~~. Where these external ~~experts may be internal auditors of the group to which the institution belongs. Where experts~~providers act as *réviseurs d'entreprises agréés*, they ~~shall~~must, in all respects, be independent from the *réviseur d'entreprises agréé* and the *cabinet de révision agréé* of the institution as well as from the group to which these persons belong.

Chapter 7. Specific requirements

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

~~43.~~ The organisational structure shall ~~be~~, in terms of legal entities (structures~~)~~), be appropriate and justified as regards the strategies and guiding principles ~~referred to in point 17 of this circular.~~

163. . 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 ~~shall~~must not impede the ~~ability~~sound governance of the institution, in particular the ability of ~~its administration and~~the management ~~bodies~~body, to effectively manage and ~~control~~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 ~~limit~~delineate the powers which it agrees to delegate to the ~~heads~~managers of the legal entities which are part of the group in order to make sure that the ~~group head~~parent undertaking can monitor their activity, on an ongoing basis, and that it is involved in any transaction of a certain importance.

~~126.~~164. The guiding principles that the Board of Directors lays down as regards the organisational structure (in terms of legal entities) shall provide notably that:

- the organisational structure ~~does not involve~~is free from any undue complexity;

- the ~~provision~~production and distribution, in a timely manner, of all ~~necessary~~ information ~~to ensure~~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 ~~composing~~which are part of the institution is documented and may be promptly provided to the Board of Directors, the authorised management, the internal control functions or the CSSF~~,~~ upon their request.

Section 7.1.1. ~~Guiding principles as regards "non-~~Complex structures and non-standard~~"~~ or ~~"~~potentially non-transparent~~"~~ activities

~~127.~~165. ~~"~~Non-standard~~"~~ or ~~"~~potentially non-transparent~~"~~ activities are those carried out through ~~special-purpose or assimilated~~complex legal entities ~~(special-purpose vehicles) (structures)~~or arrangements or in jurisdictions ~~that impede~~which lack transparency or ~~which~~ do not meet international ~~banking~~ standards.

~~44.~~ The guiding principles ~~that the~~ regarding internal governance, which the Board of Directors lays down ~~as regards internal governance,~~ shall provide ~~in particular~~, notably that ~~the~~complex structures and non-standard ~~and~~or potentially non-transparent activities are

- ~~only acceptable provided that~~ 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 ~~is confident that~~must understand the ~~inherent risks can be effectively managed;~~
- ~~controlled through processes~~usefulness of ~~approval~~these structures and ~~management of~~manage the risks ~~and management information available at the level of the authorised management and internal control functions of the institution;~~

~~128.~~166. ~~monitored, on a regular basis, in order to ensure that they remain necessary and consistent with~~ that accompany their ~~original purposes and~~establishment and their operational functioning.

- ~~monitored, on a regular basis, by the internal control functions and by the *réviseur d'entreprises agréé* of the institution.~~

~~45. Points 162 and 163 shall also apply where the institution carries out non-standard and non-transparent activities on behalf of its customers.~~

Commission de Surveillance du Secteur Financier

Sub-chapter 7.2. Management of conflicts of interest

~~129.~~167. The policy on ~~managing~~ the management of conflicts of interest shall cover all conflicts of interest, ~~with a~~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 Board of Directors.

~~130.~~168. The policy on ~~managing~~the management of conflicts of interest shall provide that all current and possible conflicts of interest ~~shall~~must be identified ~~with the aim of avoiding them~~, 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 ~~in the interest of~~so as to avoid that the institution, its counterparties and ~~pursuant to the regulatory provisions on customer protection.~~the customers suffer unjustified consequences thereof. The policy and procedures in question shall also ~~lay down~~include the procedure to be followed in case of non-compliance with ~~the~~this policy ~~in question~~.

~~131.~~169. The policy on ~~managing~~ the management of conflicts of interest shall ~~identify~~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 ~~is~~or its staff and its representatives are or may be faced ~~with and~~. It shall ~~state how these~~ take into consideration not only present situations and events which may result in conflicts of interest ~~shall be managed. In order to minimise~~, but also those in the recent past in so far as these events continue to have a potential ~~of conflicts of interest,~~impact on the institution or person concerned. The institution shall determine the materiality of the identified conflicts and shall ~~put in place appropriate segregation of duties and activities.~~decide how they must be managed.

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

~~46.~~ The policy on the management of conflicts of interest shall also determine the reporting and escalation procedures applicable within the institution. Where the staff members are or have been faced with a conflict of interest, they shall promptly inform their senior manager on their own initiative. ~~Where the senior manager notes that the conflict of interest is acceptable in view of the internal policy, s/he shall authorise it under the terms and conditions provided for in this policy. The policy in question shall also lay down the escalation procedure which determines the conflicts of interest which shall be reported to the authorised management and authorised by it.~~

~~132.~~171. The members of the authorised management and the Board of Directors, who are subject to a conflict of interest, shall promptly inform the authorised management or the Board of Directors, respectively, on their own initiative. The procedures in this regard shall provide that these members shall abstain from participating in ~~the~~ decision-making ~~processes~~ where they may have a conflict of interest or ~~which prevent them~~where they are prevented from deciding with full objectivity and independence.[18]

~~133.~~172. The internal control functions ~~are~~shall be in charge of identifying and managing conflicts of interest.

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

~~134.~~173. The ~~business relationships~~transactions with related parties ~~are~~shall be subject to the Board of ~~directors'~~Directors' approval where they have or may have, individually or on an aggregate basis, a significant and negative impact on the risk profile of the institution. ~~The rule shall also apply where, in the absence of any significant impact on each individual transaction, the influence is significant for all transactions with related parties.~~

~~135.~~174. Any material change in ~~the~~ significant transactions carried out with related parties ~~shall~~must be brought to the attention of the Board of Directors as soon as possible.

~~136.~~175. Transactions with related parties ~~shall~~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 ~~capacities~~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.

[18] *This provision is in line with ~~that~~those of ~~Article 57~~Articles 441-7 (one-tier system) and 442-18 (two-tier system) of the Law of 10 August 1915 on commercial companies ~~stating that as regards public limited companies (sociétés anonymes) and European 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 ~~board of directors conflicting~~body concerned which conflicts with that of the company, shall ~~be obliged to advise~~inform the ~~board~~body in question thereof and ~~to~~ 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~~."~~.*

~~137.~~176. Where the institution is group head, it shall consider, in a balanced way and ~~balance~~in compliance with the applicable legal provisions, the interests of all legal entities and branches which are part of the group ~~and comply with the applicable legal provisions.~~. It shall consider how these interests contribute to the common ~~purpose~~objectives and interests of the group over the long term.

Sub-chapter 7.3. New Product Approval Process

~~138.~~177. ~~"New products"~~ The new product approval process shall ~~mean any change in~~cover the development of new activities ~~(~~in terms of ~~coverage of~~products, services, markets, systems and processes or customers~~, products and services).~~ as well as their material changes and exceptional transactions.

~~47. No new activity shall be undertaken unless approved by the authorised management, all relevant parties have been heard, and the means mentioned in point 179 are available. The process in question is laid down in a new product approval process which complies with the provisions of points 177 to 180.~~

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

~~139.~~178. The new product approval process shall define, in particular, the changes in the activities subject to the approval process ~~(significant change in the activities)~~, 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 ~~approval process shall lay down the rights and obligations of all relevant parties, including the internal control functions as well as the conditions~~main issues to be ~~fulfilled for approval. These conditions~~addressed shall include regulatory compliance, accounting, pricing ~~and~~ models, the impact on risk ~~control, internal expertise, technical infrastructure and sufficient human~~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 ~~ensure~~understand and monitor the ~~entire operational processing.~~ associated risks.

~~140.~~179. Consequently, the institutions shall carefully analyse any proposed change in the activities and ensure that they have the ability to bear the risks related thereto, the technical infrastructure and sufficient and competent human resources to control these activities and the associated risks ~~related thereto.~~. The business unit ~~which requests~~requesting the change in its activities ~~is~~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 ~~institution's~~ 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. ~~With respect to their opinions, the internal control functions can rely on analyses carried out by the business units.~~

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

~~141.~~181. The internal control functions may require that a change in activities shall be deemed to be ~~significant~~material and thus be subject to the approval process.

Sub-chapter 7.4. Outsourcing

~~142.~~182. Outsourcing shall mean the complete or partial transfer of the operational ~~functions~~tasks, activities or ~~provisions of~~ services of the institution to an external service provider, whether or not ~~s/he~~it is part of the group to which the institution belongs.

~~Whereas IT outsourcing, or a chain of outsourcing exclusively composed of IT outsourcing, relies on a cloud computing infrastructure as defined in Circular CSSF 17/654, the points of sub-chapter 7.4 of this circular shall not apply and the financial professional shall comply with the requirements of Circular CSSF 17/654.~~

For the purposes of this sub-chapter, the term ~~"~~"activity"~~"~~ shall refer to the operational ~~functions~~tasks, activities and ~~provisions of~~ services mentioned in the first paragraph. Any activity that, when it is not carried out in accordance with the rules, reduces the ~~institution's~~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"~~.~~".

183. 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

~~143.~~184. Outsourcing ~~should~~must not result in non-compliance with the rules of this Circular on central administration ~~(Chapters 1 and 3).~~ .

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 ~~functions~~tasks and ~~manage~~the management of the risks associated with the outsourcing;
- ~~The data protection shall be guaranteed at all times;~~
- 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 ~~any~~the delegation of the institution's responsibility to the subcontractor~~, except as regards the obligation of professional secrecy where the subcontractor acts under Article 41(5) of the LFS;~~ ;
- The final responsibility ~~of~~for the ~~risk~~ management of risks associated with outsourcing ~~is incumbent upon~~shall lie with the ~~authorised management~~institution which is outsourcing;
- ~~The institution shall assess, in view of possible legal risks and legal obligations, whether or not the third parties concerned by this outsourcing, and in particular financial sector customers, should be informed, or their consent be obtained. In this respect, the institution shall comply with the regulations in force relating to personal data protection;~~

- The confidentiality and integrity of data and systems ~~shall~~must be controlled throughout the outsourcing chain. In particular, access to data and systems ~~shall~~must fulfil the principles of "need to know" and "least privilege", i.e. access ~~is~~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 ~~shall~~must obtain prior authorisation from the CSSF. A notification to the CSSF ~~stating~~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 ~~according to~~in accordance with Articles 29-1 to 29-6 of the LFS;
- The access of the CSSF, the *réviseur d'entreprises agréé* and the internal control functions of the institution to the information relating to the outsourced activities ~~shall~~must be guaranteed in order to enable them to issue ~~an~~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 ~~on~~of an external partner. The aforementioned opinion may be, where appropriate, ~~be~~ based on the reports of the subcontractor's external *réviseur* (auditor~~.~~).

~~144.~~185. 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 ~~evaluation~~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.

~~145.~~186. Special attention ~~should~~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~~institution's ability to meet the regulatory requirements or even to continue its activities.

~~146.~~187. Special attention ~~should~~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.

~~147.~~188. The institutions ~~shall~~must take into account the risks associated with the outsourcing ~~"~~"chains~~"~~" (where a service provider outsources part of ~~his/her~~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 CSSF with any elements proving that the sub-outsourcing process is under control.

~~148.~~189. The outsourcing policy ~~should consider~~shall take into account the impact of the outsourcing on the institution's ~~business~~activities and ~~the~~ risks ~~it faces.~~, 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 ~~include reporting~~lay down the applicable requirements regarding outsourcing to which the service providers ~~and~~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 ~~are subject~~ 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 CSSF or the challenge ~~the CSSF's~~of its supervision.

~~149.~~190. Special attention ~~should~~must be paid to the continuity aspects and the revocable nature of outsourcing. The institution ~~shall~~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 ~~clauses~~clause or service termination ~~clauses~~clause because of resolution actions or reorganisation measures or a winding-up procedure applied to the institution, as ~~provided for~~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 ~~activities~~services to a different provider or to ~~perform those activities itself~~bring them in-house whenever the continuity or quality of the service provision ~~are~~is likely to be affected.

~~150.~~191. For each outsourced activity, the institution shall designate, from among its ~~employees~~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

~~151.~~192. The institution shall implement an IT policy which covers all IT activities ~~scattered~~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 ~~procedure~~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.

~~152.~~193. The ~~IT system~~institution's policy on information systems security ~~policy of the institution should~~shall consider the ~~personal~~individual security ~~established~~implemented by its subcontractor(s~~)~~), in order to ensure ~~the~~ overall consistency.

~~153.~~194. 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

~~154.~~195. 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 ~~and~~, which exclusively ~~deals with~~processes group transactions~~, provided that~~. In case these systems ~~do not~~ include ~~any~~ readable confidential data ~~on the~~of customers~~. Otherwise~~, the institution shall ~~assess, in view of possible legal risks and legal obligations, whether or not~~ensure compliance with the provisions of Article 41(2a) of the ~~third parties concerned by this outsourcing, and in particular financial sector customers, should be informed, or their consent be obtained. In this respect, the institution shall comply with the regulations in force relating to personal data protection~~LFS.
- Abroad, from:

- any IT service provider, including from an entity of the group to which the institution belongs~~, provided that~~. In case these systems ~~do not~~ include ~~any~~ readable confidential data ~~on~~of customers~~. Otherwise~~, the institution shall ~~assess, in view of possible legal risks and legal obligations, whether or not the third parties concerned by this outsourcing, and in particular financial sector customers, should be informed, or their consent be obtained. In this respect, the institution shall comply~~ensure compliance with the ~~regulations in force relating to personal data protection~~provisions of Article 41(2a) of the LFS.

Sub-section 7.4.2.2. Consulting, development and maintenance services

~~155.~~196. 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.

~~156.~~197. Third-party subcontractors ~~other than support PFS~~ which provide consulting, development or maintenance services ~~shall~~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 ~~shall~~must ensure that the third party in question is supervised 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 production system, except interventions carried out by a support PFS as part of its mandate.~~ and that the provisions of Article 41(2a) of the LFS are complied with.

~~157.~~198. Any change in the application functionality by a third party - other than ~~the~~ changes relating to corrective maintenance - ~~shall~~must be submitted for approval to the institution prior to its implementation.

~~158.~~199. 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 ~~case~~ the ~~subcontractor defaults~~event of a subcontractor's failure, for a period compatible with a transfer of this outsourcing to another subcontractor or a ~~taking over~~takeover of the applications concerned by the institution itself.

Sub-section 7.4.2.3. Hosting services and infrastructure ownership

~~159.~~200. The IT infrastructure may be owned by the institution or be provided by the subcontractor.

Where the IT infrastructure includes readable confidential data~~, only the staff~~ of customers, the institution shall ensure compliance with the ~~support PFS or~~provisions of ~~the Luxembourg credit institution can work either in their premises or those of the financial professional without any specific supervision by the staff of the institution, provided that the service is provided under~~ Article 41(~~5~~2a) of the LFS~~ and is the subject of a service contract enabling this autonomy. Where the subcontractor is not a support PFS or a Luxembourg credit institution, the institution shall assess, in view of possible legal risks and legal obligations, whether or not the third parties concerned by this outsourcing, and in particular financial sector customers, should be informed, or their consent be obtained.~~. Otherwise, the subcontractor cannot ~~intervene~~operate on the ~~premises~~ infrastructure of the institution without being accompanied, throughout its mission, by a person of the institution in charge of IT.

~~Where the IT infrastructure does not include confidential data, express approval~~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.

~~160.~~201. 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 ~~that which provides~~the one providing IT system management services. In this case, the institution ~~shall~~must ensure that the principles ~~contained~~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.

~~161.~~202. 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~~this provider does not act as operator. If the provider has ~~no~~ physical ~~and~~or logical access to the institution's systems, the institution shall ensure compliance with the provisions of Article 41(2a) of the LFS.

~~162.~~203. 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 ~~shall~~must be controlled throughout the ~~IT~~ outsourcing chain. In particular, access to data and systems ~~shall~~must fulfil the principles of "need to know" and "least privilege", i.e. access ~~is~~shall only be granted to persons whose functions so require, ~~with~~for a specific purpose, and their privileges shall be limited to the strict necessary minimum to ~~exercise~~perform their functions. The institution shall ~~assess, in view~~ensure compliance with the provisions of ~~possible legal risks and legal obligations, whether or not the third parties concerned by this outsourcing, and in particular financial sector customers, should be informed, or their consent be obtained.~~ Article 41(2a) of the LFS.

Section 7.4.3. Additional general requirements

~~163.~~204. In order to enable the institution to assess the reliability and ~~comprehensiveness~~completeness of the data produced by the IT system as well as ~~their~~its compatibility with the accounting and internal control requirements, ~~there should be~~ one person, among its ~~employees with~~staff members, must have the ~~required~~necessary IT knowledge to understand both the impact of the programmes on the accounting system and the actions ~~taken~~performed by the third party within the context of the provided services.

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

~~164.~~205. In case of IT service provision via telecommunication, the institution ~~shall~~must ensure that:

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

~~165.~~206. The institution ~~shall~~must ensure that the capture, printing, backup, storage and archiving mechanisms guarantee the confidentiality of the data.

~~166.~~207. Outsourcing ~~shall~~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 ~~shall~~must allow keeping regular accounts in accordance with the ~~rules~~standards applicable in Luxembourg and thus respecting the form and content rules imposed by the Luxembourg accounting laws and regulations.

~~48. Where the institution operates abroad by using services of professional intermediaries (even if they are part of the group to which the institution belongs) or where it has branches or representative offices, any access by these intermediaries or representatives and employees of these offices and branches to its IT system in Luxembourg shall be approved by the CSSF.~~

Section 7.4.4. Documentation

~~167.~~208. Any outsourcing of material or non-material activities ~~or not~~, 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 Board of Directors 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).

~~168.~~209. The written documentation ~~should~~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.

~~169.~~210. 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 ~~possibility~~full opportunity to exercise their controls.

Commission de Surveillance du Secteur Financier

Chapter 8. Legal reporting

~~170.~~211. ~~Credit institutions~~The investment firms shall provide the CSSF with the ICAAP~~ report~~/ILAAP reports and ~~compliance~~the annual certificate of compliance with the requirements of this Circular issued by the authorised management ~~in accordance with point 61~~ as well as the summary reports of the internal control functions~~ in accordance with point 116 together with the draft annual accounts to be published ("VISA procedure"). Investment firms shall provide the CSSF with~~. This information ~~within the~~shall be submitted to the CSSF, at the latest, one month ~~of~~after the ordinary general meeting ~~having~~that approved the annual accounts. The relevant information ~~are to~~shall be drafted in French, German or English.

Part III. Risk management

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

Sub-chapter 1.1. Institution-wide risk management framework

Section 1.1.1. General information

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

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

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

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

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

~~49. The risks shall be assessed based on an objective and critical analysis specific to the institution. It should not exclusively rely on external assessments.~~

~~50. The institution shall explicitly reflect all the different risks in their internal governance arrangements including in particular the strategies and policies on regulatory and internal own funds and liquidity (reserves). It shall determine, in particular, its tolerance levels as regards all risks to which it is exposed.~~

The risk policy shall describe how the various risks are identified, measured, ~~reported,~~ managed, ~~limited~~monitored and ~~controlled~~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 ~~ensures~~ensure that the institution has a thorough overview of all the risks at all times.

~~The institutions~~Pursuant to the provisions of Chapter 2 of Part III of this Circular, the risk policy shall ~~have an internal limit and alert threshold system~~take due account of concentration risks.

~~1.~~4. The capital and liquidity policy implementing the strategy of the Board of Directors in respect of ~~all their risks.~~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 ~~toward related parties are to be dealt with internally~~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.

~~***toward third parties.***~~ ***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.

~~2.~~6. The institution must explicitly reflect all the different risks in its internal governance arrangements ~~shall apply to them in their entirety.~~including, in particular, the strategies and policies on risks and on capital and liquidity reserves.

~~**Sub-chapter 1.2. Risk measurement**~~

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

~~3.~~8. The risk measurement and reporting arrangements ~~should~~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.

~~4.~~9. The decisions on risk-taking and risk strategies and ~~risk~~ policies ~~should~~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.

~~5.~~10. In general, the risk measurement techniques implemented by an institution ~~should~~shall be based on choices, assumptions and approximations. There is no absolute measurement.

Commission de Surveillance du Secteur Financier

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

Chapter 2. Concentration risk

~~6.~~11. Concentration risk results, in particular, from large ~~(~~concentrated~~)~~ exposures to customers ~~or~~, counterparties or service providers, respectively, ~~or~~ groups of customers ~~or related~~, counterparties or related service providers, including related parties, ~~on~~to countries or sectors (industries) as well as ~~on~~to specific products or markets (intra-risk concentration). These exposures ~~may be assets and liabilities items~~are not necessarily limited to balance sheet items or off-balance sheet items~~, but concentration risk does not necessarily refer 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 ~~concentration~~concentrations may result in economic and financial losses as well as in a significant and negative impact on the risk profile of the institution.

~~51. Points 211 to 215 shall apply, in particular, to~~ Concentration risk~~.~~

~~**Chapter 3. Credit risk**~~

~~**Sub-chapter 3.1. General principles**~~

~~52. Each credit risk-taking shall~~ must be subject to ~~a written analysis which should cover at least the debtor's creditworthiness, the repayment plan~~particular vigilance and ~~the borrower's repayment ability throughout the maturity of the debt. The institutions shall take into account the overall debt level of the borrower.~~

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

~~53. Each credit risk-taking shall be subject to a predetermined decision-making process which should also involve a body separate from the business function.~~

~~54. For low credit risk-taking, institutions may establish a grant-making process which should enable them to monitor this risk-taking as a whole without~~

necessarily going through the decision-making processes and individual analyses as referred to in points 221 and 222.

The institutions are in charge of internally defining the concept of "low" credit risk for the purposes of the first paragraph. This definition is based, in particular, on the institution's ability to manage, bear and control these risks.

55. The institutions shall have clear policies 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.

56. Each decision to restructure the credit shall be subject to the decision-making process laid down in points 221 to 223. The institutions shall maintain a list including all the restructured credits.

The restructuring measures are those which are related to deterioration of the creditworthiness of the debtor. They shall include in particular the granting of extensions, postponements, renewals or changes in credit terms and conditions, including the repayment plan.

57. The institutions shall have sound arrangements to identify and manage past due commitments. Past due commitments are commitments whose contractual maturity dates set for the payment of principal and/or interests have expired.

The institutions shall have sound arrangements for the identification, management and provisioning of "doubtful" commitments. These refer to all commitments "in default" within the meaning of Part VII, Sub-section 3.4.2.2, of Circulars CSSF 06/273 and CSSF 07/290 which define the default in terms of significant delays in payment (exceeding 90 days) or indication of unlikeliness to pay.

58. The institutions shall maintain a list of the doubtful commitments on the debtor or group of related debtors. These commitments shall be subject to periodic and objective review which shall enable the institution to acknowledge and carry out the impairment and provisions of assets as required.

~~**Sub-chapter 3.2. Residential mortgages to individuals**~~

~~**Specification:**~~

~~For institutions operating on the domestic market, there is generally a concentrated exposure on the Luxembourg real estate market. A significant market downturn, which is very difficult to predict, would be likely to~~ effort as it may jeopardise the financial stability of ~~these institutions and to have an adverse impact on the image of the Luxembourg financial centre as a whole. Consequently, institutions shall implement prudent policies as regards the granting of mortgages pursuant to Sub-chapter 3.1 and point 228. Moreover, institutions shall have sufficient capital in order to face adverse developments in the residential real estate market. The requirements prescribed in point 229 aim to strengthen the financial stability of these institutions through duly risk-adjusted regulatory capital requirements. These requirements strengthen the current rules included in Circular CSSF 06/273 according to the lessons learnt from the recent financial crisis episodes. Thus, in accordance with the first indent of point 229, institutions using the standardised approach for credit risk can, from now on, only apply the preferential risk weight of 35% to the parts of their mortgages whose loan-to-value ratio (LTV) is below 80% (mortgages "whose value of the property is at least 25% higher than that of the exposure"). Consequently, a mortgage which fulfils all qualifying criteria of Section 2.2.7.1 of Part VII of Circular CSSF 06/273 (weighted retail exposure of 75%) and the criteria of Section 2.2.8.1 of Part VII of this circular (preferential risk weight of 35%) except for the new criteria 41, point d) which limits the LTV to 80% shall be, from now on, weighted for the purposes of determining the regulatory capital requirements at (0.8/LTV)*35%+((LTV-0.8)/LTV)*75% instead of 35%. The part of the mortgage exceeding 80% of the value of the real estate object is to be weighted according to the underlying exposure class. In this particular instance, the exposure shall comply with all criteria for retail exposures and the risk weight shall consequently be 75%. For the purpose of determining the LVT, the institutions may take into account all risk mitigation factors - direct personal contribution from the borrower or even the intervention of third parties by way of contributions, security interests or guarantees or collateral under the conditions provided for in Part IX of Circular CSSF 06/273 ("recognition of credit risk mitigation techniques"). For institutions using the internal ratings-based approach and in accordance with the second indent of point 229, the absolute floor for the loss ratio in the event of default shall remain at 10% after 31 December 2012.~~ the institution.

~~These institutions shall also ensure that their regulatory capital adequacy is subject to a stress test which shall at least fall within the parameters referred to in the third indent of point 229.~~

~~59. The institutions shall apply a prudent credit granting policy which aims to safeguard their financial stability regardless of the developments in the residential real estate market. This policy shall focus on a healthy ratio between the amount of the credit granted and the value of the securities held (loan-to-value), including the underlying property.~~

~~60. Part VII of Circular CSSF 06/273 shall be amended as follows:~~

- ~~Under point 41, point d), the phrase ", by a substantial margin," shall be replaced by "by at least 25%";~~
- ~~Under point 176, the beginning of the sentence "Until 31 December 2012," shall be deleted. In the title of paragraph 3.2.4.2.3., the word "transitional" shall be deleted;~~
- ~~Under point 257, the third sentence "The test to be employed shall be meaningful and reasonably conservative, considering at least the effect of mild economic recession scenarios" shall be replaced by "The test to be employed shall be relevant and reflect the consequences of a severe but plausible economic recession scenario". Finally, a second paragraph with the following content shall be added at the end of point 257: "For the purposes of the first paragraph, the stress test on the retail exposures secured by residential property requires an increase of minimum 50% of the PDs and a LGD of at least 20%".~~

~~**Sub-chapter 3.3. Credit to real estate developers**~~

~~61. Each real estate development project funding shall 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 funding. When this time limit is exceeded, the file shall be automatically classified under the list of restructured credits (cf. point 225) and the unpaid interests shall be fully paid.~~

~~The real estate development funding shall not only be based on the developer's reputation. It shall 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 exposure (Part XVI of Circular CSSF 06/273), 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 shall be in healthy proportion to their regulatory capital.~~

Chapter ~~4~~3. Risk transfer pricing

~~7.~~12. The ~~institution~~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 ~~tolerance~~appetite and the principle of sound and prudent business management.

~~8.~~13. The pricing mechanism shall be approved by the authorised management and ~~supervised~~monitored by the risk control function. The transfer prices ~~shall~~must be transparent and communicated to the relevant ~~employees.~~staff members. The comparability and consistency of the internal transfer ~~price~~pricing systems used within the group ~~shall~~must be ensured.

~~9.~~14. The institution shall establish a complete and effective internal transfer ~~price~~pricing system for liquidity. This system shall include all liquidity costs, benefits and risks.

Chapter ~~5. Private~~4. Wealth management and associated activities (“private banking~~”)~~” activities)

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

~~10.~~16. These institutions shall have sound ~~arrangements~~processes to ensure that the business relationships with their customers comply with the ~~contracts entered into~~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.~~17. ~~The~~These institutions shall have sound arrangements to ensure compliance with the ~~customers'~~customers' risk profiles, for the ~~purpose~~purposes, in particular, of fulfilling the requirements arising from the MiFID regulations.

~~12.~~18. ~~The~~These institutions shall have sound arrangements in place to ensure the communication of accurate information to the customers on the state of their assets. The issue and distribution of account statements and any other information on the state of assets ~~shall~~must be separated from the business function.

~~13.~~19. ~~Transfers~~The physical inflows and ~~withdrawals~~outflows of cash, securities or other valuables ~~(for instance cash and bearer instruments) shall~~must be carried out and ~~controlled~~overseen by a function separated from the business function.

~~14.~~20. Any entry and amendment of customers' identification data ~~shall~~must be carried out ~~and controlled~~or overseen by ~~an~~ a function that is independent ~~function~~ from the business function.

~~15.~~21. If a customer purchases ~~an exchange-traded~~ 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.

~~16.~~22. ~~The~~These institutions ~~shall~~must have sound arrangements in respect of ~~credit and bank overdraft within~~ control of credits (or loans) granted in the context of the ~~private banking activities.~~provision of ancillary services referred to in point (2) of Section C of Annexe II of the LFS. The financial guarantees covering these credits ~~shall~~must be sufficiently diversified and liquid. For the ~~purpose~~purposes of having an adequate security margin, prudent discounts ~~shall~~must be applied according to the nature of the financial ~~collateral. The~~guarantees. These institutions ~~shall~~must have an early warning system independent from the business function which ~~should organise~~organises the monitoring of the financial ~~collateral's~~guarantees' value and ~~trigger~~triggers the liquidation process of the financial guarantees. It ~~shall~~must ensure that the liquidation process is triggered in good time, and in any case before the value of the ~~collateral~~guarantees becomes lower than the credit. Contracts with customers ~~shall~~must clearly describe the procedure triggered in the event of inadequacy of the guarantees.

Chapter ~~6~~5. Exposures to shadow banking entities

~~17.~~23. This chapter shall only apply to institutions to which Part Four (Large exposures) of ~~Regulation (EU) No 575/2013~~the CRR applies, in accordance with the level of application set out in Title II of Part One~~, Title II~~ of said regulation.

Sub-chapter ~~6~~5.1. Implementation of sound internal control principles

~~18.~~24. ~~The~~These institutions shall put in place an internal framework for the identification, management, ~~control~~monitoring and mitigation of the risks arising from the exposures to shadow banking entities[19] in accordance with EBA/GL/2015/20.

[19] *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".*

~~19.~~25. ~~The~~These institutions shall apply a materiality threshold to identify the exposures to shadow banking entities. In accordance with EBA/GL/2015/20, any individual exposure to a shadow banking entity that is equal to or in excess of 0.25%[20] of the institution's eligible capital[21], after taking into account the effect of the credit risk mitigation and exemptions[22], ~~shall~~must be taken into consideration and cannot be deemed as low exposure.

~~20.~~26. ~~The~~These institutions shall ensure that any possible risks for the institution as a result of their various exposures to shadow banking entities are adequately taken into account within the institution's Internal Capital Adequacy Assessment (ICAAP) and capital planning.

Sub-chapter ~~6~~5.2. Application of quantitative limits

~~21.~~27. ~~The~~These institutions shall limit their exposures to shadow banking entities in accordance with one of the two approaches (principal approach or fallback approach) as defined in ~~Guidelines~~ EBA/GL/2015/20.

~~22.~~28. In accordance with the principal approach, ~~the~~these institutions ~~should~~must set an aggregate limit to their exposures to shadow banking entities relative to their eligible capital.

~~23.~~29. When setting an aggregate limit to exposures to shadow banking entities, each ~~institution should~~of these institutions must take into account:

- its business model, risk management framework~~,~~ and risk appetite;
- the size of its current exposures to shadow banking entities relative to its total exposures and relative to its total exposure to regulated financial sector entities;
- interconnectedness ~~between~~, on the one hand, between shadow banking entities and, on the other hand, between shadow banking entities and the institution.

~~24.~~30. Independently of the aggregate limit, and in addition to it, these institutions ~~should~~must set tighter limits on their individual exposures to shadow banking entities.

~~25.~~31. When setting those limits, as part of their internal assessment process, ~~the~~these institutions ~~should~~must take into account:

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

[21] *Within the meaning of point (71) of Article 4(1) of ~~Regulation (EU) No 575/2013~~the CRR.*

[22] *i) Credit risk mitigating effects in accordance with Articles 399 and 403 of ~~Regulation (EU) No 575/2013~~the CRR;*

ii) Exemptions provided for in Articles 400 and 493(3) of ~~Regulation (EU) No 575/2013~~the CRR.

- 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 ~~between~~, 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.

~~26.~~32. If these institutions are not able to apply the principal approach as set out above, their aggregate exposures to shadow banking entities ~~should~~must be subject to the limits on large exposures in accordance with Article 395 of ~~Regulation (EU) No 575/2013~~the CRR (hereinafter the "fallback approach").

~~27.~~33. The fallback approach ~~should~~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 ~~should~~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~~5.1 of this part, but cannot gather sufficient information to enable them to set out appropriate limits as set out in ~~Section 6~~Sub-chapter 5.2~~.1~~, they ~~should~~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 ~~Section 6~~Sub-chapter 5.2~~.1 should~~ must be applied to the remaining exposures to shadow banking entities.

Chapter ~~7. Asset encumbrance~~

~~62. This chapter only applies to credit institutions.~~

~~63. The credit 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 should take into account each credit institution's business model, the Member States in which they operate, the specificities of the funding markets and the macroeconomic situation. The policies should be approved in accordance with the provisions of point 19.

64. The credit institutions shall have in place a general monitoring framework that provides timely information, at least once a year, to the authorised management and the board of directors 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 additional encumbrance resulting from stress scenarios (contingent encumbrance).

65. The credit 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.

Specification:

Risk encumbrance shall be monitored through additional tables aiming at reporting encumbered assets, which will supplement Commission Implementing Regulation (EU) No 680/2014, in accordance with the CRR on prudential requirements for credit institutions. Draft provisional templates were published by the European Banking Authority on 24 July 2014 (EBA/ITS/2013/04/rev1).

Chapter 8<u>6</u>. Interest rate risk

<u>Sub-chapter 6.1.</u> <u>Interest rate risk</u> arising from non-trading book activities

66. CRR institutions[23], When implementing Article 14 (Interest <u>rate</u> risk arising from non-trading book activities) of CSSF Regulation N° <u>RCSSF</u> 15-02 relating to the supervisory review and evaluation process that applies to CRR institutions, <u>, the CRR investment firms</u> shall comply with the guidelines published by the European Banking Authority in this respect.[24]

[24] *"Guidelines on the management of interest rate risk arising from non-trading activities" (EBA/GL/2015/08) available on the EBA's website: https://www.eba.europa.eu/-/cba-updates-guidelines-on-interest-rate-risk-arising-from-non-trading-activities.*

Commission de Surveillance du Secteur Financier

~~Investment firms which are not CRR investment firms do not fall within this chapter.~~

~~67. These guidelines include high-level guidelines and detailed guidelines which target the following three areas: internal capital allocated to the interest rate risk in the banking book ("IRRBB 1"), measurement of this risk ("IRRBB 2" and "IRRBB 3") and internal governance arrangements with regard to interest rate risk in the banking book ("IRRBB 4.1" and "IRRBB 4.2").~~

~~Part IV. Entry into force, transitional measures and repealing provisions~~

~~68. This circular is applicable as from 1 July 2013.~~

~~By way of derogation from the first paragraph, the following provisions are applicable as from 1 January 2014:~~

- ~~Section 4.1.2 (Composition and qualification of the board of directors);~~
- ~~Section 4.1.4 relating to the specialised committees, with the exception of the audit committee;~~
- ~~Point 32 (Prohibition to combine the mandates of chairman of the board of directors and authorised manager);~~
- ~~The need to lay down in writing the guidelines provided for in indents 4 to 8 of point 17.~~

~~69. Circulars IML 93/94 and CSSF 10/466 shall be repealed as from 1 July 2013.~~

~~70. Circulars IML 95/120, IML 96/126, IML 98/143, CSSF 04/155 and CSSF 05/178 shall no longer be applicable to credit institutions and investment firms as from 1 July 2013.~~

~~71. Successive updates:~~

- ~~Circular CSSF 13/563 transposing the EBA guidelines on the eligibility of the directors, authorised managers and persons in charge of the key functions dated 22 November 2012 (Guidelines on the assessment of the suitability of members of the management body and key function holders – EBA/GL/2012/06) as well as the ESMA guidelines of 6 July 2012 on certain aspects of the MiFID compliance function requirements – ESMA/2012/388).~~

  ~~The aforementioned guidelines are available on the EBA's website) and ESMA's website ().~~

- ~~Circular CSSF 14/597 transposing the recommendation of the European Systemic Risk Board (ESRB) on funding of credit institutions (ESRB/2012/2) – recommendation B on the implementation of a risk management framework as regards asset encumbrance.~~

  ~~The aforementioned recommendation is available on the ESRB's website ().~~

~~28.~~34. ~~Circular CSSF 16/642 implementing the EBA Guidelines on~~ EBA Guidelines on the management of interest rate risk arising from non-trading book activities ~~–~~ (EBA /GL/~~2015/08.~~2018/02).

- ~~Circular CSSF 16/647 implementing the EBA guidelines relating to the 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).~~

~~The above-mentioned guidelines~~Sub-chapter 6.2. Corrections to modified duration for debt instruments

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

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

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

Commission de Surveillance du Secteur Financier

Part IV. Entry into force

This Circular repeals and replaces Circular CSSF 12/552, as amended by Circulars CSSF 13/563, CSSF 14/597, CSSF 16/642, CSSF 16/647, CSSF 17/655 and 20/750, for investment firms and shall apply as from 1 January 2021.

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

Claude WAMPACH
Director

Marco ZWICK
Director

Jean-Pierre FABER
Director

Françoise KAUTHEN
Director

Claude MARX
Director General

~~Annexe~~

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

Commission de Surveillance du Secteur Financier

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Circular CSSF 20/758
Central administration, internal governance, risk management

Main changes (compared to Circular CSSF 12/552*)

*Repealed for investment firms

7 December 2020

cssf
Commission de Surveillance
du Secteur Financier

Circular CSSF 20/758: main reasons for the introduction of a new circular intended specifically for investment firms

- The regulatory framework applicable to credit institutions is increasingly diverging from the one applicable to investment firms.
- Maintaining one single circular which covers different entities and activity areas has become difficult to manage.
- More flexible requirements regarding central administration, internal governance and risk management for investment firms pursuant to the principle of proportionality.

Circular CSSF 20/758: main reasons for the amendments in comparison to Circular CSSF 12/552

- No significant update of the part concerning governance since 2012
- Required implementation of EBA and ESMA guidelines (GL)
  - **EBA/GL/2017/11 on internal governance**
  - **EBA/GL/2017/12 on the assessment of the suitability of members of the management body and key function holders**
  - EBA/GL/2018/02 on interest rate risks arising from non-trading book activities
  - EBA/GL/2016/09 on corrections to modified duration for debt instruments
- GL which are not covered:
  - EBA/GL/2019/02 on outsourcing arrangements
- Correction of individual errors and additional clarifications

Circular CSSF 20/758 in the European context

- EBA/GL/2017/11 and EBA/GL/2017/12: two guidelines particularly important for this update.
- Circular CSSF 20/758 is applicable to all investment firms.
- Circular CSSF 20/758 takes into account the Luxembourg context.

Circular CSSF 20/758: main amendments

Terminology:

- The definitions of “Board of Directors” and “authorised management” of Circular CSSF 20/758 were adapted following guidelines EBA/GL/2017/11

The management body in its supervisory function + the management body in its management function = **The management body**

- The management body in its supervisory function = **the Board of Directors (one-tier structure) or the supervisory board (two-tier structure)**
- The management body in its management function = **the authorised management**

- The definition of significant investment firms henceforth refers to systemically important investment firms (Article 59-3 of the Law of 5 April 1993 on the financial sector, as amended) and, where appropriate, to other investment firms defined by the CSSF.

Circular CSSF 20/758: main amendments (continue)

- Structure of the document: slight changes
  - Renumbering of paragraphs inside the parts
  - Rearrangement of some sections to facilitate the reading
- Scope
  - Applicable to all investment firms and indirectly applicable to financial holding companies or mixed financial holding companies.
  - Circular CSSF 12/552 remains applicable in its entirety to credit institutions and in part to professionals performing lending operations.
- Consideration of environmental, social and governance (ESG) risk factors with a view to ensuring viability of the business model.

Circular CSSF 20/758: main amendments (continue)

- Board of Directors: independent members and diversity
  - In principle, at least one member of the Board of Directors of a CRR investment firm must be considered as “independent”.
  - Within significant institutions or institutions whose shares are admitted to trading on a regulated market, a sufficient number of independent members of the Board of Directors is required.
  - Enhanced provisions regarding diversity.
- Chairperson of the Board of Directors: The chairperson of the Board of Directors shall not exercise executive functions within the institution. Thus, the mandates of authorised manager and chairperson of the Board of Directors cannot be combined and the chairperson of the Board of Directors cannot be another staff member of the institution.

Circular CSSF 20/758: main amendments (continue)

- Specialised committees: The significant institutions must put in place an audit committee, risk committee, nomination committee and a remuneration committee.
- Outsourcing of the internal audit: Only authorised for operational tasks. The Board of Directors of the investment firm shall remain ultimately responsible for outsourcing the internal audit operational tasks.
- Chief Risk Officer (CRO): In significant institutions, the CRO shall be a member of the authorised management who is independent and individually responsible for the risk control function. Possibility to be member of the senior management due to the principle of proportionality, provided there is no conflict of interest.

Circular CSSF 20/758: main amendments (continue)

- Deletion of Chapter 3 of Part III on “Credit risk” (only applicable to credit institutions and professionals performing lending operations)
- Deletion of Chapter 7 of Part III on “Asset encumbrance” (only applicable to credit institutions)

Circular CSSF 20/758: additional clarifications concerning...

- criteria to take into account the principle of proportionality and their necessary documentation and approval by the Board of Directors
- the code of conduct, the risk and the compliance culture
- the documentation of the organisation, the functioning and decisions of the Board of Directors and authorised management
- the specialised committees: the composition, the combination (for reasons of proportionality) and the functioning of the specialised committees
- the internal control functions:
  - the organisation of the internal control functions and the application of the principle of proportionality to these functions
  - the role, organisation and importance of the risk control function

Circular CSSF 20/758 Central administration, internal governance, risk management

Main changes (compared to Circular CSSF 12/552*)

*Repealed for investment firms

7 December 2020

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