

# COMMISSION de SURVEILLANCE du SECTEUR FINANCIER

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

Luxembourg, 19 March 2013

To all credit institutions, investment firms and professionals performing lending operations\*

## CIRCULAR CSSF 13/563

### **Re: Update of Circular CSSF 12/552 on the central administration, internal governance and risk management**

Ladies and Gentlemen,

This circular amends Circular CSSF 12/552 by including the EBA (European Banking Authority) guidelines dated 22 November 2012 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 (European Securities and Markets Authority) guidelines dated 6 July 2012 on certain aspects of the MiFID compliance function requirements (ESMA/2012/388).

The ESMA guidelines on certain aspects of the MiFID compliance function requirements set out considerations relating to the tasks and responsibilities of the compliance function arising from MiFID. These guidelines are divided into "general guidelines" and "supplementary guidelines" which provide additional clarification on the general guidelines. The ESMA general guidelines parallel to a large extent the general rules on the compliance function laid down in Chapter 6 of Circular CSSF 12/552 and do not represent an innovation in its own right for credit institutions and investment firms. Where the institutions implement the compliance function relating to the provision of investment services in accordance with MiFID, they shall take into account the "additional guidelines" laid down in the document ESMA/2012/388.

The EBA guidelines on the assessment of the suitability of members of the management body and key function holders provide clarification on Chapter 4 of Circular CSSF 12/552 and in particular Sections 4.1.1., 4.1.2. and 4.2.2. as regards the guiding principles to be laid down by the management body in respect of the selection, assessment, corrective measures and the documentation of the nominations to key functions, including the mandates as members of the management body of a credit institution or an investment firm. Each credit institution and investment firm is in charge of listing these key functions, based on the principle of proportionality. However, the

---

\* For professionals performing lending operations, as defined under Article 28-4 of the law of 5 April 1993 on the financial sector, only Chapter 3 of Part III remains applicable. This circular does not in any way change the obligations incumbent upon these professionals.

CSSF considers that the definition of the key functions covers at least the members of the management body and the holders of the three internal control functions.

1. Circular CSSF 12/552 is amended in accordance with the annexe.

The annexe in question includes the amendments brought by Circular CSSF 12/552 in "track changes" in order to ease the reading and understanding.

2. The amendments brought by this circular to Circular 12/552 shall enter into force in accordance with the provisions of item 241 of Part IV of Circular CSSF 12/552. As a result, new requirements arising from the guideline ESMA/2012/388 shall apply as from 1 July 2013. The new requirements arising from the guideline EBA/GL/2012/06 shall apply as from 1 July 2013, except for the assessment of the professional skills and personal qualities of the members of the management body which shall be subject to the provisions of Circular CSSF 12/552 as from 1 January 2014.

#### COMMISSION DE SURVEILLANCE DU SECTEUR FINANCIER

Claude SIMON  
Director

Simone DELCOURT  
Director

Jean GUILL  
Director General

#### **Annexe**

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

Luxembourg, 11 December 2012

To all credit institutions, investment firms and professionals carrying on lending operations<sup>1</sup>

**CIRCULAR CSSF 12/552 as amended by**  
**Circular CSSF 13/563**

**Re: Central administration, internal governance and risk management**

Ladies and Gentlemen,

Articles 5 (1a) and 17 (1a) of the law of 5 April 1993 on the financial sector require credit institutions and investment firms to have robust internal governance arrangements, which include a clear organisational structure with well defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks 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 and promote sound and effective risk management, as well as control and security mechanisms of their IT systems.

In the past, as a result of the regulatory developments at international level and the local needs, the CSSF specified the procedures for implementing these articles in various circulars. The addition of new circulars transposing the guidelines of 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) 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 internal governance in one single circular. This circular reflects the above-mentioned EBA and BCBS guidelines supplementing them by the additional provisions included in Circulars IML 96/126, IML 98/143, CSSF 04/155, CSSF 05/178 and CSSF 10/466<sup>2</sup>.

---

<sup>1</sup> As regards professionals carrying on 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.

<sup>2</sup> 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.

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.

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.<sup>3</sup>

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 EBA guidelines dated 2 September 2010 on concentration risk ("CEBS Guidelines on the management of concentration risk under the supervisory review process (GL31)") and the guidelines dated 27 October 2010 on liquidity pricing ("Guidelines on Liquidity Cost Benefit Allocation"). Moreover, the circular highlights the basic principles of prudence in the field of credit granting and private wealth management.

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.](#)

The circular is divided into four parts: the first part 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.

[The boxes which appear in the circular include the remarks and clarifications which serve as guidance to update the requirements included in this circular.](#)

---

<sup>3</sup> Circulars IML 95/120, IML 96/126, IML 98/143 and CSSF 05/178 shall remain applicable for PFS other than investment firms. These circulars together with Circular CSSF 04/155 shall remain applicable for payment institutions and electronic money institutions.

## Table of contents

<b>Part I.</b>	<b>Definitions and scope</b> .....	<b>5</b>
Chapter 1.	Definitions .....	5
Chapter 2.	Scope.....	5
<b>Part II.</b>	<b>Central administration and internal governance</b>	
	<b>arrangements</b> .....	<b>7</b>
Chapter 1.	Central administration.....	7
Chapter 2.	Internal governance arrangements .....	7
Chapter 3.	General characteristics of "robust" central administration and internal governance arrangements .....	9
Chapter 4.	Board of directors and authorised management.....	10
Sub-chapter 4.1.	Board of directors .....	10
Section 4.1.1.	Responsibilities of the board of directors .....	10
Section 4.1.2.	Composition and qualification of the board of directors .....	13
Section 4.1.3.	Organisation and functioning of the board of directors .....	14
Section 4.1.4.	Specialised committees.....	15
Sub-section 4.1.4.1.	Audit committee.....	16
Sub-section 4.1.4.2.	Risk committee .....	17
Sub-chapter 4.2.	Authorised management .....	18
Section 4.2.1.	Responsibilities of the authorised management.....	18
Section 4.2.2.	Qualification of the authorised management .....	20
Section 4.2.3.	Specific (risk, capital and liquidity) policies .....	21
Chapter 5.	Administrative, accounting and IT organisation.....	22
Sub-chapter 5.1.	Organisation chart and human resources .....	22
Sub-chapter 5.2.	Administrative and technical infrastructure.....	23
Section 5.2.1.	Administrative infrastructure of the business functions .....	23
Section 5.2.2.	Financial and accounting function .....	23
Section 5.2.3.	IT function .....	24
Section 5.2.4.	Internal communication and whistleblower arrangements .....	25
Section 5.2.5.	Crisis management arrangements .....	26
Sub-chapter 5.3.	Internal documentation .....	26
Chapter 6.	Internal control.....	27
Sub-chapter 6.1.	Operational controls.....	27
Section 6.1.1.	Day-to-day controls carried out by the operating staff .....	27
Section 6.1.2.	Ongoing critical controls .....	27
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 .....	28
Sub-chapter 6.2.	Internal control functions.....	29
Section 6.2.1.	General responsibilities of the internal control functions .....	29
Section 6.2.2.	Characteristics of the internal control functions .....	30
Section 6.2.3.	Execution of the internal control functions' work .....	31
Section 6.2.4.	Organisation of the internal control functions .....	32
Section 6.2.5.	Risk control function .....	33
Sub-section 6.2.5.1.	Specific responsibilities and scope of the risk control function.....	34
Sub-section 6.2.5.2.	Organisation of the risk control function.....	35
Section 6.2.6.	Compliance function.....	35
Sub-section 6.2.6.1.	Compliance charter.....	36
Sub-section 6.2.6.2.	Specific responsibilities and scope of the compliance function .....	36
Sub-section 6.2.6.3.	Organisation of the compliance function.....	38
Section 6.2.7.	Internal audit function.....	39
Sub-section 6.2.7.1.	Internal audit charter .....	39
Sub-section 6.2.7.2.	Specific responsibilities and scope of the internal audit function .....	40

Sub-section 6.2.7.3.	Execution of the internal audit work .....	41
Sub-section 6.2.7.4.	Organisation of the internal audit function .....	42
Chapter 7.	Specific requirements .....	43
Sub-chapter 7.1.	Organisational structure and legal entities (Know-your-structure).....	43
Section 7.1.1.	Guiding principles as regards "non-standard" or "non-transparent" activities .....	44
Sub-chapter 7.2.	Management of conflicts of interest .....	44
Section 7.2.1.	Additional requirements relating to the conflicts of interest involving related parties.....	45
Sub-chapter 7.3.	New Product Approval Process .....	45
Sub-chapter 7.4.	Outsourcing.....	46
Section 7.4.1.	General outsourcing requirements .....	46
Section 7.4.2.	Specific IT outsourcing requirements .....	48
Sub-section 7.4.2.1.	IT system management/operation services .....	48
Sub-section 7.4.2.2.	Consulting, development and maintenance services.....	49
Sub-section 7.4.2.3.	Hosting services and infrastructure ownership .....	49
Section 7.4.3.	Additional general requirements.....	50
Section 7.4.4.	Documentation.....	51
Chapter 8.	Legal reporting.....	51
<b>Part III.</b>	<b>Risk management</b> .....	51
Chapter 1.	General principles as regards risk measurement and risk management.....	51
Sub-chapter 1.1.	Risk management.....	51
Sub-chapter 1.2.	Risk measurement.....	52
Chapter 2.	Concentration risk.....	52
Chapter 3.	Credit risk .....	53
Sub-chapter 3.1.	General principles .....	53
Sub-chapter 3.2.	Residential mortgages to individuals .....	54
Sub-chapter 3.3.	Credit to real estate developers .....	55
Chapter 4.	Risk transfer pricing.....	55
Chapter 5.	Private wealth management ("private banking").....	56
<b>Part IV.</b>	<b>Entry into force, transitional measures and repealing provisions</b> .....	56

## 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 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 a board of supervisors, the latter shall assume the responsibilities that this circular assigns to the "board of directors";
- 2) "authorised management" shall mean the persons referred to in Articles 7 (2) and 19 (2) of the law of 5 April 1993 on the financial sector. These persons are referred to as "authorised managers";
- 3) "institution" shall mean an entity as defined in Chapter 2 of Part I;
- 4) "key function": any function the exercise of which may have a significant influence on the conduct or monitoring of activities. These key functions include at least the directors, authorised managers and the persons in charge of the three internal control functions in accordance with point 105 (i.e. the risk control function, the compliance function and the internal audit function);
- ~~4)5)~~ "LFS" shall mean the law of 5 April 1993 on the financial sector;
- ~~5)6)~~ "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

2. This circular shall apply to credit institutions and investment firms governed by Luxembourg law, including their branches as well as Luxembourg branches of credit institutions and 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 money laundering and terrorist financing, markets in financial instruments and liquidity – Luxembourg branches of credit institutions and investment firms originating from a Member State of the European Economic Area shall establish central administration and internal governance arrangements as well as risk management arrangements which are comparable to those provided for in this circular.

In respect of professionals carrying on lending operations as defined in Article 28-4 of the LFS, only Chapter 3 of Part III of this circular shall apply.

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

3. The circular shall apply to institutions on a single and consolidated basis.

Where there are legal entities, whether consolidated or not, whose 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. The circular shall then apply to the "group" as a whole, the various legal entities that are part of it, including their possible 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 the organisational and operational structure of the institution, the implementation of this circular enables the institution to have complete control over its activities and the risks to which it is or may be exposed, irrespective of the location of these activities and risks.

4. Proportionality shall apply to the implementing measures which institutions take pursuant to this circular having regard to the nature, scale and complexity of the 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 have in place enhanced central administration and internal governance arrangements. These arrangements include, for example, the establishment of specialised committees pursuant to Section 4.1.4. However, for institutions whose activity is less diversified, significant or complex, the principle of proportionality could be applied less strictly. Thus, these institutions may operate properly within the meaning of this circular with compliance and risk control functions assumed on a part-time basis (cf. points 129 and 141), with an outsourced 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 application of the principle of proportionality is limited in particular by the principle of segregation of duties under which the duties and responsibilities shall be assigned so as to avoid conflicts of interest involving the same person (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 of duties within the authorised management is done in compliance with the principle of segregation of duties, joint liability shall be maintained. In application of the principle of proportionality, where an 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). Regardless of the organisation adopted, 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. Central administration and internal governance arrangements**

### **Chapter 1. Central administration**

5. Institutions shall have a robust central administration in Luxembourg, consisting of a "decision-making centre" and an "administrative centre". The central administration which comprises, in a broad sense, the management, execution and control functions shall enable the institution to retain control over all of its activities.
6. The concept of "decision-making centre" does not only comprise the authorised management's activities pursuant to Articles 7 (2) and 19 (2) of the LFS but also that of the persons in charge of the various business, support and control functions or the various business units (services, departments or positions) existing within the institution.
7. The administrative centre shall include in particular a sound administrative, accounting and IT organisation which ensures, at all times, proper administration of securities and assets, proper 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).
8. Where the institution is the group head pursuant to point 3, the central administration shall enable the institution to concentrate all management information necessary to manage, monitor and control, on an ongoing basis, the activities of the group in its registered 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 management information. The concept of management information shall be understood in the broadest possible sense, including financial information and the prudential reporting.

### **Chapter 2. Internal governance arrangements**

9. Internal governance is a limited but crucial component of the corporate governance framework, focusing 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 other stakeholders.

Internal governance shall ensure in particular sound and prudent business management, including the risks inherent in them. In order to achieve this objective, the institutions shall establish 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.

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 include the four levels of control provided for in point 100.

10. 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 decision-making powers, reporting and functional links and segregation of duties which are clearly 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. These mechanisms 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 systems (Sections 5.2.1 to 5.2.3, Sub-chapters 5.3 and 7.4);
- 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;
- 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 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 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 of crisis, including a business recovery plan. These arrangements shall meet the requirements set out in Section 5.2.5.

11. The institutions shall promote an internal risk and control culture in order to ensure that all 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.

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

12. 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 security, in particular as regards information systems;
- are reliable and operate on an ongoing basis ("robustness"). Pursuant to the principle of continuity, institutions 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;
- 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 its parts ("consistency");
- are comprehensive ("comprehensiveness"). In respect of risk, comprehensiveness shall mean that all risks shall be included within the scope of the internal governance arrangements. This scope is not (necessarily) limited to the sole (consolidated) prudential or accounting scope; it shall enable the institution to have a thorough overview of all its risks, in terms of their economic substance, taking into account 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.

13. 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.

14. 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.

15. In order to ensure and maintain the soundness 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 should consider all internal and external changes which may have a significant adverse effect on the soundness of

these arrangements as a whole and on the risk profile and in particular the institution's ability to manage and bear its risks.

16. Institutions shall publish the key elements of their internal governance arrangements in compliance with the rules governing Part XIX of Circular CSSF 06/273 ("Pillar 3"). This publication shall comprise 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 and its expected development in a clear, objective and relevant manner.

## **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**

17. The board of directors shall have the overall responsibility for the institution. It shall ensure execution of activities and preserve business continuity by way of sound central administration and internal governance arrangements pursuant to the provisions of this circular. To this end, in compliance with the legal and regulatory provisions and after having heard the authorised management and the persons in charge of the internal control, and for the purpose of protecting the institution and its reputation, the board of directors shall approve and lay down in writing, notably
  - the business strategy (business model) of the institution taking into account the institution's long-term financial interests, solvency and liquidity situation;
  - the institution's risk strategy, including the risk tolerance and the guiding principles governing the risk identification, measurement, reporting, management and monitoring;
  - the strategy of the institution with respect to regulatory and internal own funds and liquidity;
  - the guiding principles of a clear and consistent organisational and operational structure which governs in particular the creation and maintenance of legal entities (structures) by the institution as well as guiding principles as regards information systems, including the security aspect, and internal communication 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 escalation, settlement and sanctions the purpose of which is to ensure that any behaviour which does not comply with the applicable rules shall be 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 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

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;

- the guiding principles applicable to business continuity management and crisis management arrangements and
- the guiding principles on the appointment and succession of individuals with key functions in the institution, ~~including as director and authorised manager and including the eligibility criteria to access these functions~~, as well as the procedures governing the composition, responsibilities, organisation and operation of the board of directors.<sup>4</sup> [The guiding principles governing the appointment and succession of individuals with key functions in the institution provide that, in this regard, the institution shall comply with the requirements of this circular, the prudential authorisation procedure of the key function holders as published on the CSSF's website as well as the guidelines published by the EBA on 22 November 2012 \(Guidelines on the assessment of the suitability of members of the management body and key function holders – EBA/GL/2012/06\).](#)

---

<sup>4</sup> 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.

18. 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 the board of directors.
19. The board of directors shall monitor the implementation by the authorised management of its internal governance strategies and guiding principles. To this end, it shall in particular approve the policies laid down by the authorised management pursuant to point 18.
20. The board of directors shall critically assess and approve, at regular intervals, and at least once a year, the internal governance arrangements of the institution. These assessments and 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 board of directors shall, in particular, assess and approve:

- the adequacy of the risks incurred with the institution's ability to manage these risks and the internal and regulatory own funds and liquidity reserves, taking into account the strategies and guiding principles laid down by the board of directors, the existing regulations and in particular 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 responsibilities set out in Sub-chapter 4.2. In this context, the board of directors shall ensure, in particular, that the authorised management promptly and effectively

implements the required corrective measures 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;

- the adequacy of the organisational and operational structure. The board of directors shall 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 links and interconnections between them 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 sound and prudent business management which is transparent and free from undue complexity, and that it remains justified in relation to the set objectives. This requirement shall apply, in particular, to "non-standard" or "non-transparent" activities;
- the efficiency and effectiveness of the internal control mechanisms put in place by the authorised management.

The assessments in question may be prepared by the 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 reports of the internal control functions (point 116) which the board of directors is called upon to approve on this occasion.

21. The board of directors is in charge of promoting an internal risk culture which heightens the awareness of the institution's staff as regards the requirements of sound and prudent risk management and which fosters a positive attitude vis-à-vis 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 of these functions are executed in compliance with recognised standards. Moreover, the board of directors approves the internal audit plan pursuant to point 151.

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

#### **Section 4.1.2. Composition and qualification of the board of directors**

23. The number of the members of the board of directors shall be sufficient and the board of directors as a whole shall be properly composed so that it can fully meet its responsibilities. The adequacy of the composition of the board of directors refers in

particular to professional skills (knowledge, understanding and experience), as well as personal qualities of the members of the board of directors. Moreover, each member shall demonstrate his/her professional standing. The guiding principles governing the election and succession of the directors explain and determine the abilities deemed necessary to ensure appropriate composition and qualification of the board of directors.

24. The board of directors as a whole shall have appropriate skills with regard to the nature, scale and complexity of the activities and the organisation of the institution.

The board of directors, as a collective body, shall fully understand all 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 understanding of the other significant activities of the institution.

25. The members of the board of directors shall ensure that their personal qualities enable them to properly perform their director's mandate, with the required commitment, availability, objectivity, critical thinking and independence. 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 of the institution, with the exception of staff representatives).

The members of the board of directors make sure that their director's mandate is and remains compatible with any other positions 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.

26. The terms and conditions of the directors' mandates shall be laid down so as to enable the board of directors to fulfil its responsibilities on an ongoing basis and effectively. The renewal of the existing directors' mandates shall in particular be based on their past performance. Continuity in the functioning of the board of directors shall be ensured.

27. 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 which enable the members of the board of directors to update and develop their required skills.

#### **Section 4.1.3. Organisation and functioning of the board of directors**

28. The board of directors shall meet on a regular basis in order to effectively perform its duties.

29. The work of the board of directors shall be documented in writing. This documentation shall include the agenda of the meeting, the minutes of the meeting as well as the decisions and measures taken by the board of directors.

30. The board of directors shall assess, on a regular basis, the procedures governing the board of directors, its mode of functioning and its work in order to improve them, to

ensure effectiveness and to verify whether the applicable procedures are complied with in practice.

31. The chairman of the board of directors is in charge of promoting, within the board of directors, a culture of informed and contradictory discussion and to propose the election of independent directors. An independent director 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<sup>5</sup> - relationship with the institution, its controlling shareholder or the management of either.

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

32. The mandates of authorised manager and chairman of the board of directors cannot be combined.

#### **Section 4.1.4. Specialised committees**

33. For the purpose of increasing its effectiveness, the board of directors may be assisted by specialised committees notably in the fields of auditing, risk, remuneration, human resources ([notably through the intervention of a nomination committee of the key function holders](#)) as well as internal governance, professional ethics and compliance where the 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 to provide the board of directors with critical assessments in respect of the organisation and operation of the institution in the aforementioned areas in order to enable the members of the board of directors to fulfil their supervisory mission and to take on their responsibilities pursuant to this circular.
34. The board of directors shall lay down in writing: the mandate, composition and working procedures of the specialised committees. Pursuant to these procedures, the specialised committees shall be able to request any document and information they deem necessary to fulfil their mission. Moreover, the procedures 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 the work of the specialised committees.
35. The board of directors shall ensure that the various committees effectively interact and report to the board of directors on a regular basis. The board of directors cannot delegate its decision-making powers and responsibilities to specialised committees pursuant to this circular.
36. 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.
37. 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.

---

<sup>5</sup> Including an employment relationship.

#### **Sub-section 4.1.4.1. Audit committee<sup>6</sup>**

38. The purpose of the audit committee is to assist the board of directors in the areas of financial information, internal control, including internal audit as well as the control by the *réviseur d'entreprises agréé*.

39. The CSSF recommends larger institutions to establish an audit committee in order to facilitate effective supervision of the activities by the board of directors.

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 of the members of 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.

40. The functioning of the audit committee, in particular in terms of frequency and duration of the meetings, shall be determined in relation to its mandate and its mission to assist the board of directors.

41. The audit committee shall confirm the internal audit charter (point 144). 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.

42. 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.

43. The audit committee shall deliberate, on a regular basis, on<sup>7</sup>:

- the follow-up of the financial reporting process;
- the state of the internal audit and compliance with the rules set in this respect in this circular on the basis, in particular, of the internal audit function reports;
- the quality of the work carried out by the internal audit function and 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 rules of professional ethics applicable to the audit area. In this respect, the audit committee shall critically analyse and assess the audit plan, the reports on

---

<sup>6</sup> 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.

<sup>7</sup> 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.

- 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 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;
- the actions to be taken in case of 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.

44. 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.

#### **Sub-section 4.1.4.2. Risk committee**

45. The purpose of the risk committee is to assist the board of directors in its mission to assess the adequacy between the risks incurred, the institution's ability to manage these risks and the internal and regulatory own funds and liquidity reserves.
46. The CSSF recommends larger institutions as well as institutions with a higher or more complex risk profile to create a risk committee in order to facilitate the effective risk control by the board of directors.
47. The risk committee can involve the authorised management as well as the persons in charge of the internal control in its work. These persons can attend the committee's meetings; they are not members of it.
48. The risk committee shall confirm the specific policies of the authorised management in accordance with Section 4.2.3.
49. 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.
50. The risk committee shall deliberate, on a regular basis, on:
- the state of the risk management and compliance with the prudential rules laid down in this respect;
  - the quality of the work carried out by the risk control function and compliance with the rules laid down 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 appropriate follow-up without undue delay by the authorised management of the recommendations of the risk control function;
- the actions to be taken in case of problems, shortcomings and irregularities identified by the risk control function.

51. The risk committee shall advise the board of directors on the definition of the overall risk strategy of the institution, including its current and future risk tolerance.

## **Sub-chapter 4.2. Authorised management**

### **Section 4.2.1. Responsibilities of the authorised management**

52. The authorised management is in charge of the effective, sound and prudent day-to-day business (and inherent risk) management. This management shall be exercised in compliance with the strategies and guiding principles laid down by the board of directors and the existing regulations, taking into account and safeguarding the institution's long-term financial interests, solvency and liquidity situation. The decisions taken by the authorised management in these areas shall be duly documented.

53. Pursuant to Articles 7 (2) and 19 (2) of the LFS, the members of the authorised management shall be authorised to effectively determine the business direction. Consequently, where management decisions are taken by management committees which are larger than solely the authorised management, the authorised management shall be part of it and have a veto.

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

54. The authorised management shall implement through internal written 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 shall ensure that the institution has the necessary internal control mechanisms, technical infrastructures and human resources to ensure sound and prudent business (and inherent risk) management within the context of robust internal governance arrangements pursuant to this circular.

55. Pursuant to point 18, the authorised management shall define an internal code of conduct applicable to all persons working in the institution. It shall ensure its correct application on the basis of controls carried out by the compliance and internal audit functions on a regular basis.

56. The authorised management shall have an absolute 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 links and interconnections between them as well as the risks related thereto. It shall ensure that the management information is available in due time at all decision-making and control levels of the institution and legal structures which are part of it.

57. In its day-to-day management, the authorised management shall take into account 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) identified through the internal control functions and the *réviseur d'entreprises agréé* by taking into account their recommendations 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 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, human resources and technical infrastructure) required in this respect. The internal control functions are in charge of monitoring 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 authorise time extensions for the implementation of the corrective measures.

The institution shall establish a similar procedure, approved by the board of directors, which applies 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.

58. The authorised management shall verify the implementation and compliance with internal policies and procedures. Any violation of internal policies and procedures shall result in prompt and adapted corrective measures.
59. The authorised management shall verify the soundness of the central administration and internal governance arrangements on a regular basis. It shall adapt the internal policies and procedures in light of the internal and external, current and anticipated changes and the lessons learnt from the past.
60. The authorised management shall inform the internal control functions of any significant changes 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 inform, 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 and compliance with the internal governance arrangements, including the state of compliance and internal control as

well as the ICAAP report<sup>8</sup> on the situation and management of the risks and the internal and regulatory own funds and liquidity (reserves). This information shall relate in particular to the state of internal control. 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 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.

62. Where the authorised management becomes aware that the central administration and internal governance arrangements no longer enable sound and prudent business management or that the risks incurred are or will no longer be properly borne by the institution's ability to manage these risks, by the regulatory or internal own funds or 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).
63. Notwithstanding the overall responsibility of the members of the authorised management (cf. point 72), it shall designate at least one of its members to 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 shall be, in particular, in charge of developing the organisation chart and 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. The member in question shall also be in charge of the provision and publication of accounting information intended for third parties and the transmission of periodic information to the CSSF. Thus, s/he shall ensure that the form and content of this information comply with the legal rules and the rules 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.

64. The institutions shall provide 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 the appointments and revocations of these persons by giving the grounds for revocation.

#### **Section 4.2.2. Qualification of the authorised management**

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

---

<sup>8</sup> Cf. point 26 of Circular CSSF 07/301.

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

66. 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.

67. 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

68. 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 made available to all relevant staff in an easily accessible manner.
69. The organisation chart shall show for the different (business, support and control) functions as well as for the different business units (services, departments or positions) their structure and the reporting and business lines between them and with the authorised management and the board of directors.
70. The task description to be filled in by the operating staff shall explain the function, powers and responsibility of each officer.
71. Without prejudice to point 72, the organisation chart and task description shall be established based on the principle of segregation of duties. Pursuant to this principle, the duties and responsibilities shall be assigned so as to avoid that they are incompatible for the same person. The goal pursued is to avoid conflicts of interest and to prevent through a peer review environment a person from making mistakes and irregularities which would not be identified.
72. Pursuant to Articles 7 (2) and 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 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 organise this segregation so as to avoid conflicts of interest. Thus, it is advisable not to assign the functions relating to risk-taking and independent control of these risks to the same member of the authorised management. Similarly, the authorised manager who himself/herself ~~serves as performs the function of~~ Chief Compliance Officer pursuant to point 141, cannot, at the same time, be responsible for the internal audit function. Where, due to the small size of the institution, several duties and responsibilities have to be assigned to the same person, this grouping shall be organised so that it does not prejudice the objective pursued by the segregation of duties.
73. The institution has an ongoing training programme which shall ensure that the staff members as well as the board of directors and the authorised management remain qualified and include the internal governance arrangements as well as their own roles and responsibilities in this regard.
74. Each employee shall annually take at least ten consecutive personal days off. It must be assured that the employee 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. Administrative and technical infrastructure**

75. 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**

76. 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**

77. 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.

78. 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.

79. 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.

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

81. 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.

82. 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.

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.

83. 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.

84. 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**

85. 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.

86. 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.

87. 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**

88. 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.
89. 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.
90. 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**

91. 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.
92. 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.
93. 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**

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

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 accessible to the institution's staff.

95. The description of the procedures for the execution of activities (transactions) concerns the following points:
  - successive and logical stages of the transaction processing, from initiation to documentation storage;
  - flow of the documents used;
  - periodic reviews to be carried out, as well as the means to ensure that they have been carried out.

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

96. 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 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.

97. The files, working papers and control reports of the internal control functions, experts and subcontractors referred to in Sub-chapter 6.2 as well as the long-form reports drawn up by the *réviseurs d'entreprises agréé* shall be kept during five years in the Luxembourg institution in order to enable the institution to track the controls

carried out, the problems, shortcomings or irregularities identified as well as the recommendations and conclusions. The CSSF as well as the *réviseur d'entreprises agréé* shall always be able to access these documents.

98. 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.

## **Chapter 6. Internal control**

99. The internal control is 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 and requirements of the CSSF are met.<sup>9</sup>

100. A suitable internal control environment requires 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 of the administrative processing of transactions as specified in Section 6.1.2;
- controls carried out by the members of the authorised management on the activities or functions which fall under their direct responsibility as specified in Section 6.1.3;
- controls carried out by the internal control functions as defined in Sub-chapter 6.2.

### **Sub-chapter 6.1. Operational controls**

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

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

#### **Section 6.1.2. Ongoing critical controls**

102. This category of controls shall include *inter alia*:

---

<sup>9</sup> 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, institutions whose asset management activity and service activities related in particular to the administration of UCIs are significant, define adequate internal control mechanisms for these activities, in particular in the field of discretionary management, processing of held mails, safekeeping of securities of third parties (depository bank), bookkeeping and net asset value calculation of investment funds.

- hierarchical control;
- validation (for example dual signature, codes of access to specific features) regarding 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 of the existence of the value of the assets and liabilities, on a regular basis, in particular by means of verification of inventories;
- reconciliation and confirmation of accounts;
- monitoring of the accuracy and completeness of the data transmitted by the persons in charge 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 transactions concluded, in particular, in respect of their price, scale, possible guarantees to be received or provided, profits generated and losses incurred, the amount of possible brokerage fees.

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

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

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

The areas requiring particular attention by these persons are *inter alia*:

- risks associated with the activities and functions for which they are directly responsible;
- 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;
- compliance with the policies and procedures established by the authorised management pursuant to point 18;
- compliance with established budgets: review of actual achievements and gaps;
- compliance with limits (in particular based on exception reports),
- characteristics of the transactions, in particular their price, their individual profitability;
- evolution of the overall profitability of an activity.

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

## **Sub-chapter 6.2. Internal control functions**

104. 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 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). These policies which describe the fields of intervention directly related to each internal control function shall clearly define the responsibilities for the common fields of intervention and the objectives as well as the independence, objectivity and permanence of the internal control functions.
105. 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 ~~as soon as possible~~ [in compliance with the prudential authorisation procedure of the key function holders as published by the CSSF on its website by stating the reasons for this revocation.](#)

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**

106. The main purpose of the internal control functions is 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 the organisational and operational structure, strategies, activities and risks of the institution as well as as regards the applicable legal and regulatory requirements and to report directly to the authorised management as well as the board of directors pursuant to point 116. They shall provide the authorised management and the board of directors with the opinions and advice they deem necessary in order to improve the central administration and internal governance arrangements of the institution.
107. 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 they consider that effective, sound or prudent business management is challenged, the persons responsible for

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.

108. Where the institution is the group head, its internal control functions supervise and control the internal control functions of the group. The internal control functions of the institution shall ensure that the shortcomings, irregularities and risks identified throughout the whole group are reported to the local management bodies and boards of directors as well as the authorised management and board of directors of the institution pursuant to point 116.

### **Section 6.2.2. Characteristics of the internal control functions**

109. The internal control functions shall be permanent and independent functions each with sufficient authority. The persons in charge of these functions shall have direct access right to the board of directors or its chairman or, where appropriate, the chairmen of 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:

- 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, which the internal control functions shall 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 business units of the institution they control) deemed necessary to fulfil their missions.

110. The staff of the internal control functions or third parties (cf. point 118) acting on behalf of these functions shall be objective in carrying out their work.

In order to ensure objectivity, the persons in charge of the internal control functions shall exercise independent thinking and judgement: they should not make their own judgement conditional upon that of other persons including, in particular, those controlled.

Objectivity also requires that conflicts of interest are avoided.

111. In order to ensure the effectiveness of the internal control functions, its members shall individually and collectively possess high professional skills in the field of banking and financial activities and applicable standards. This competence shall be assessed by taking into account both the nature of the missions of the associates and the complexity and diversity of the activities carried out by the institution in order to enable thorough coverage of the activities and risks. This individual

competence shall 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 adapted to each of the associates.

In addition to their high professional experience, the persons in charge of the internal control functions, who take on such a position for the first time, shall have the theoretical knowledge that enables them to effectively perform this function.

112. In order to guarantee the execution of the tasks assigned to them, the internal control functions shall have the necessary and sufficient human resources, infrastructure and budgets, pursuant to the principle of proportionality (point 4). The budget shall be sufficiently flexible to reflect an adaptation of the missions of the control functions in response to changes of the institution's risk profile. These provisions are compatible with the outsourcing of the internal audit function and the use of internal control functions to external experts pursuant to points 117 and 118.
113. The internal control framework shall cover the whole institution within the limits of its respective competences. It shall include the non-standard and non-transparent activities referred to in Section 7.1.1.
114. Each institution shall take the necessary measures to ensure that the members of the internal control functions perform their functions with integrity and discretion.

### **Section 6.2.3. Execution of the internal control functions' work**

115. The internal control functions shall document the work carried out in accordance with the assigned responsibilities, in particular in order to allow tracking the interventions as well as the conclusions reached.
116. The internal control functions shall report in writing on a regular basis and, if necessary, on an ad hoc basis to the authorised management and, where appropriate, to the specialised committees. These reports shall concern the follow-up of the recommendations, problems, shortcomings and irregularities identified in the past as well as the new problems, shortcomings and irregularities identified. Each report shall specify the risks related thereto as well as their seriousness (measurement of 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. As regards the activities, each summary report shall include a statement to the authorised management of the main recommendations on (existing or emerging) problems, significant shortcomings and irregularities since the last report, 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 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, the nature and level of reliance on external experts pursuant to point 118 as well as any problems which may have occurred in this context. This report

shall be submitted to the board of directors and, where appropriate, the specialised committees for approval; it is submitted to the authorised management for information.

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

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

#### **Section 6.2.4. Organisation of the internal control functions**

117. Outsourcing the compliance function and risk control function is not authorised. The internal audit function can be outsourced by smaller institutions whose risk profile is low and non-complex, subject to the conditions laid down in point 118 and Sub-section 6.2.7.4. This kind of outsourcing is, in principle, not acceptable for institutions with agencies, branches or subsidiaries.

118. The provisions of point 112 do not exclude the possibility for the internal control functions to use the expertise or technical resources of third parties for certain aspects. This use is governed by an internal procedure which shall, in particular, enable the authorised management and the board of directors to assess the dependencies and risks for the institution arising from a significant use of these third parties.

The authorised management shall select these third parties ("experts") on the basis of an analysis of suitability between the institution's needs and the specific services and competences offered by these third parties. The selected expert shall be independent from the institution's *réviseur d'entreprises agréé* and the *cabinet de révision agréé* as well as from the group to which these persons belong.

The use of an external expert shall be based on a written mandate. The expert shall carry out his/her work in compliance 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 be placed under the dependence of the person in charge of the internal control function covering the controlled area. This person supervises the experts' work.

119. Pursuant to point 3, the internal control functions of an institution shall also be put in place at the level of the group, legal entities and branches composing it. These constituent parts shall each have their own internal control functions, taking into account the principle of proportionality as indicated in point 4.

120. Within the branches of the institution, the internal control functions depend, from a hierarchical and functional point of view, on the control functions of the group head to which they belong and to which they report.

As regards the subsidiaries, the internal control functions 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 to the local management and supervisory bodies but, in summarised form, to the internal control functions of the parent institution which analyses them and reports the points to be noted in accordance with point 116.

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

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.

121. The principles of this circular do not exclude that, for Luxembourg institutions which are or not branch or subsidiary 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**

##### **Important comments:**

1. Reference is made to points 9, 17, 21, 33, 45 to 51, 57, 104 to 121, 147 and 179 also relating to 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.

122. The risk control function is entrusted to a dedicated department composed of one or several persons.
123. 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.

The field of intervention of the risk control function shall also include the risks associated with the complexity of the 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**

124. The risk control function shall ensure that the regulatory and internal risk limits are compatible with the strategies, activities and organisational and operational structure of the institution. It shall monitor compliance with these limits and the proper application of the escalation procedure provided for in case of breach and shall ensure that the breaches are remedied as soon as possible.
125. The risk control function shall ensure that the authorised management and the board of directors receive a 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 between these risks and the own funds and liquidity (reserves) and the institution's ability to manage these risks in normal times and in times of stress. This assessment shall be based, in particular, on the stress test programme in accordance with Circular CSSF 11/506. It shall also include an assessment as regards the adequacy between the risks incurred and the strategies laid down by the board of directors, in particular regarding the risk tolerance.
126. The risk control function shall ensure that the terminology, methods and technical resources used for the risk anticipation, identification, measurement, reporting, management and monitoring are consistent and effective.
127. 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 be validated by qualitative (expert) judgements.

The risk control function shall compare its ex-ante possible risk assessments with the ex-post risks on a regular basis in order to improve the adequacy of its assessment methods (back-testing).

128. 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 in order to guarantee that the risks relating thereto remain controlled.

### Sub-section 6.2.5.2. Organisation of the risk control function

129. 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.

It is acceptable for the member of the authorised management designated as being directly in charge of the risk control function to assume himself/herself the position of Chief Risk Officer.

### Section 6.2.6. Compliance function

#### **Important 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.

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

131. The aim of the compliance function is to anticipate, identify and assess the compliance risks of an institution as well as to assist 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 risk aspects, in connection with all activities of the institution.

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

[The institutions which provide investment services within the meaning of the LFS shall implement a compliance function which complies with the ESMA guidelines of 6 July 2012 \(Guidelines on certain aspects of the MiFID compliance function requirements \(ESMA/2012/388\)\).](#)

#### **Specification:**

[This circular includes "general guidelines" included in the document ESMA/2012/388 and applies them to all activities of the institution, including the provision of investment services. Where they implement these requirements in relation to the investment services within the meaning of the LFS, the institutions shall take into account the "supporting guidelines" set out in the document ESMA/2012/388.](#)

### **Sub-section 6.2.6.1. Compliance charter**

132. The terms of operation of the compliance function in terms of objectives, responsibilities and powers are 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.
133. The compliance charter shall at least:
- define the position of the compliance function in the organisation chart of the institution by 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 all activities of the institution including those of its branches and subsidiaries in Luxembourg and abroad and to access to all documents, materials, minutes of the consultative and decision-making bodies of the institution, to meet all persons working in the institution, to the extent required to fulfil its mission;
  - 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 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 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 brought to the attention of all staff members of the institution, including those who work in branches abroad and subsidiaries in Luxembourg and abroad.

134. The compliance charter shall be updated as soon as possible in order to take into account the changes in the applicable standards affecting the institution. Any changes shall 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 brought to the attention of all staff members.

### **Sub-section 6.2.6.2. Specific responsibilities and scope of the compliance function**

135. For the purpose of reaching the objectives set, the responsibilities of the compliance function shall 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 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 ~~them in order to determine~~ their significance ~~and as well as~~ the possible

consequences. [The compliance risk classification so determined shall 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 network of the group at international level.
- 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 day-to-day tasks. These rules shall be properly reflected in the instructions, procedures and internal controls in areas directly related to compliance. In drawing up these rules, the compliance function shall take into account, as far as necessary for the institution in question, the code of conduct laid down in the internal governance arrangements.
- The areas directly related to the compliance function are typically the fight against money laundering and terrorist financing, the prevention regarding market abuse and personal transactions, the integrity of the financial instruments markets, the protection of the customers' and investors' interests, the data protection and observance of professional secrecy, the avoidance and management of conflicts of interest, the prevention of the use of the financial sector by third parties to circumvent their regulatory obligations and the management of the compliance risk related to cross-border activities. In 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 or even frauds. This list is not exhaustive. 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 above may not be covered by the compliance function. In this case, it is understood that the compliance risk is to be covered by the other internal control functions in accordance with a compliance policy clearly defining the competences 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 and verification that the other areas which do not directly fall within its competence 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.

136. The compliance function shall verify compliance with the compliance policy and procedures on a regular basis and is 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 respect of the compliance risk controls as

well as the verification of the procedures and instructions, the provisions of this circular do not prevent the compliance function from taking into account the internal audit work.

137. The compliance function shall centralise all information on the compliance problems (*inter alia* infringements of standards, non-compliance with procedures or conflicts of interest) identified by the institution.

Insofar as it did not obtain this information on 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, correspondence from the supervisory authority).

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

139. 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. To this end, it shall also develop an ongoing training programme and ensure its implementation.

140. The Chief Compliance Officer is 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 also in charge of the transmission of any information or statement to these authorities.

#### **Sub-section 6.2.6.3. Organisation of the compliance function**

141. Where, pursuant to 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.

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 application of the provisions of this circular and the proper performance of the compliance function remain assured.

Subject to specific authorisation by the CSSF, the member of the authorised management 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

### **Important 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.

142. The internal audit function is entrusted with the internal audit department, composed of one or several persons.
143. 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**

144. The terms of operation of the internal audit function in terms of objectives, responsibilities and powers shall be laid down by 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 at least:

- define the position of the internal audit function in the organisation chart of the institution by 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 branches abroad and subsidiaries in Luxembourg and abroad, to access all documents, instruments, 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 be drawn from the audit missions;
- define the relationships with the compliance and risk control functions;
- establish 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 of the internal audit function;

- establish the right for the Chief Internal Auditor to directly and on his/her own initiative contact the chairman 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 recognised professional standards<sup>10</sup>;
- 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 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 be updated as soon as possible to take into account the changes that have occurred. All changes shall be approved by the authorised management, confirmed, where appropriate, by the audit committee and ultimately approved by the board of directors. They are brought to the attention of all staff members.

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

In order not to challenge their independence of judgement, the persons responsible for the internal audit cannot be in charge of the preparation or establishment of elements of the central administration and internal governance arrangements. This principle does 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 be ensured, where possible, and it should be avoided that the auditors hired within the institution control 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**

146. In general, the internal audit function shall review and assess whether the central administration and internal governance arrangements are adequate and operate effectively. In this respect, the internal audit function shall assess *inter alia*:
- monitoring of compliance with the laws and regulations as well as the prudential requirements imposed by the CSSF;
  - internal control's efficiency and effectiveness;
  - adequacy of the administrative, accounting and IT organisation;
  - safeguarding of the securities and assets;
  - adequacy of the segregation of duties and of the execution of transactions;

---

<sup>10</sup> Such as for example the International Professional Practices Framework (IPPF) of the Institute of Internal Auditors (IIA)

- accurate and complete registration of the transactions and the provision of accurate, complete, relevant and understandable information available without delay to the board of directors, specialised committees and, where appropriate, 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 procedures governing the 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;
  - operation and effectiveness of the compliance and risk control functions (Sections 6.2.5 and 6.2.6).
147. Where there is, within an institution, a separate department in charge of the control or supervision of a specific activity or function, the existence of such a department does not discharge the internal audit department from its responsibility to control 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 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.
148. Further to points 119 and 120, the establishment of a local internal audit function in the subsidiaries of the institution does not discharge the internal audit of the group head from carrying out on-site inspections on these local internal audit functions.
149. 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**

150. 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 of the internal audit function for a period of several years (in general three years). Its purpose is to cover all activities and functions, taking into account 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. The plan should consider the opinions issued by the board of directors and, 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 and requests) and shall also reflect the developments and innovations provided for as well as the risks which may arise therefrom.
151. The plan shall be discussed with the authorised management and submitted to the authorised management and approved by it, confirmed, where appropriate, by 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 developments and emergencies. Any adaptation is to be formally approved by the authorised management and, where appropriate, the audit committee. 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 significantly changed.

152. 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 and risk.

The internal audit plan shall also provide for the adequate and sufficiently frequent coverage, within a period of several years, of important or complex activities which represent a significant potential risk, including a reputational risk. It shall focus on the risk of execution errors and the risk of fraud.

153. Where the internal audit department of the parent undertaking of the Luxembourg institution carries out on-site inspections on its subsidiary, on a regular basis, it is recommended for reasons of effectiveness, that, insofar as possible, the Luxembourg institution coordinates its internal audit plan with that of the parent undertaking.
154. The internal audit department shall inform the authorised management and, where appropriate, the audit committee on the implementation of the internal audit plan.
155. 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.
156. Each mission shall be the subject to a written report of the internal audit department, in general, intended for the supervised persons, the authorised management as well as - possibly in summarised form - 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 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**

157. The institution which, in line with point 117, decides to outsource the internal audit function, shall submit a written request to the CSSF. This request shall include the information necessary for its assessment, including, in particular, the name of the external expert (natural person) who will take on the internal audit function of the institution.

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.

158. In case of use of an external expert for certain aspects in accordance with point 118, this expert shall carry out his/her work under the internal audit plan of the institution by following a work programme, by producing detailed documentation on his/her work and by drafting the reports for each mission. These reports are to be drafted in French, German or English and to be delivered to the Chief Internal Auditor, the authorised management, where appropriate, the audit committee and the board of directors according to point 116.
159. Pursuant to point 118, the external experts may be internal auditors of the group to which the institution belongs. Where experts act as *réviseurs d'entreprises agréés*, they shall, in all respects, be independent from the *réviseur d'entreprises agréé* and the *cabinet de révision agréé* of the institution as well as the group to which these persons belong.

## **Chapter 7. Specific requirements**

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

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

It shall enable and promote effective, sound and prudent business management. It shall not impede the ability of the institution, in particular of its administration and management bodies, to effectively manage and control the activities (and the risks) of the institution and the different legal entities which are part of it.

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

161. 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 undue complexity;
  - the provision and distribution in a timely manner of all necessary information to ensure 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 the institution is documented and may be promptly provided to the board of directors, authorised management, internal control functions or the CSSF, upon their request.

### **Section 7.1.1. Guiding principles as regards "non-standard" or "non-transparent" activities**

162. "Non-standard" or "non transparent" activities are those carried out through special-purpose or assimilated legal entities (special purpose vehicles) (structures) or in jurisdictions that impede transparency or which do not meet international banking standards.
163. The guiding principles that the board of directors lays down as regards internal governance shall provide in particular that the non-standard and non-transparent activities are
  - only acceptable provided that the institution is confident that the inherent risks can be effectively managed;
  - controlled through processes of approval and management of risks and management information available at the level of the authorised management and internal control functions of the institution;
  - monitored, on a regular basis, in order to ensure that they remain necessary and consistent with their original purposes and
  - monitored, on a regular basis, by the internal control functions and by the *réviseur d'entreprises agréé* of the institution.
164. Points 162 and 163 shall also apply where the institution carries out non-standard and non-transparent activities on behalf of its customers.

### **Sub-chapter 7.2. Management of conflicts of interest**

165. The policy on managing conflicts of interest shall cover all conflicts of interest, with a particular attention 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 the authorised management and members of the board of directors.
166. The policy on managing conflicts of interest shall provide that all current and possible conflicts of interest shall be identified with the aim of avoiding them. Where conflicts of interest remain, the policy in this respect shall lay down the procedures to be followed in order to report and manage them in the interest of the institution and pursuant to the regulatory provisions on customer protection. The policy in question shall also lay down the procedure to be followed in case of non-compliance with the policy in question.
167. The policy on managing conflicts of interest shall identify the main sources of conflicts of interest - potentially affected relationships and activities as well as all internal and external parties involved - which the institution is or may be faced with and shall state how these conflicts of interest shall be managed. In order to minimise the potential of conflicts of interest, the institution shall put in place appropriate segregation of duties and activities.
168. 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.

169. 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 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 from deciding with full objectivity and independence.<sup>11</sup>
170. The internal control functions are in charge of identifying and managing conflicts of interest.

### **Section 7.2.1. Additional requirements relating to the conflicts of interest involving related parties**

171. The business relationships with related parties are subject to the board of directors' approval where they have or may have 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.
172. Any material change in the significant transactions carried out with related parties shall be brought to the attention of the board of directors as soon as possible.
173. Transactions with related parties shall 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 of the institution from a regulatory or internal point of view;
  - exceed the risk management and control capacities of the institution;
  - are contrary to sound and prudent management principles in the interest of the institution.
174. Where the institution is group head, it shall consider and balance 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 and interests of the group over the long term.

### **Sub-chapter 7.3. New Product Approval Process**

175. "New products" shall mean any change in the activities (in terms of coverage of markets and customers, products and services).
176. 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.

---

<sup>11</sup> This provision is in line with that of Article 57 of the law of 10 August 1915 on commercial companies stating that as regards public limited companies (*sociétés anonymes*) and European companies "any director having an interest in a transaction submitted for approval of the board of directors conflicting with that of the company, shall be obliged to advise the board thereof and to cause a record of his statement to be included in the minutes of the meeting. He may not take part in these deliberations."

177. The new product approval process shall define in particular the changes in the activities subject to the approval process (significant change in the activities) as well as the implementation of the approval process, including the responsibilities.
178. The approval process shall lay down the rights and obligations of all relevant parties, including the internal control functions as well as the conditions to be fulfilled for approval. These conditions shall include compliance, pricing and risk control, internal expertise, technical infrastructure and sufficient human resources to ensure the entire operational processing.
179. 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 risks related thereto. The business unit which requests the change in its activities is 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 the institution's ability to bear, manage and control the risks inherent in the planned activities. The compliance risk inherent in new products shall 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. The internal control functions may require that a change in activities shall be deemed to be significant and thus be subject to the approval process.

#### **Sub-chapter 7.4. Outsourcing**

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

For the purposes of this sub-chapter, the term "activity" shall refer to the operational functions, 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 ability to meet the regulatory requirements or to continue its operations as well as any activity necessary for sound and prudent risk management shall be deemed to be "material".

##### **Section 7.4.1. General outsourcing requirements**

182. Outsourcing should 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 and manage the risks associated with the outsourcing;
- The data protection shall be guaranteed at all times;

- 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 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 the risk management associated with outsourcing is incumbent upon the authorised management which is outsourcing;
  - The institution shall assess, in view of possible legal or other risks, whether or not the third parties concerned by this outsourcing, in particular customers, should be informed;
  - Data confidentiality shall be guaranteed at all times, unless explicit consent is given by the customer or the owner of the data or his/her proxy, on the basis of an informed opinion on the purpose of this outsourcing, the specific nature of the final goal, the content of the provided information, the recipient and location as well as of the sustainability;
  - The institution which intends to outsource a material activity shall obtain prior authorisation from the CSSF;
  - 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 be guaranteed in order to enable them to issue an 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 national law, have the power to perform on-site inspections on an external partner. The aforementioned opinion may, where appropriate, be based on the reports of the subcontractor's external auditor.
183. The outsourcing institution shall base its decision to outsource on a prior and in-depth analysis demonstrating that it does not result in the relocation of the central administration. This analysis shall include at least a detailed description of the services or activities to be outsourced, the expected results of the outsourcing and an in-depth evaluation of the risks of the outsourcing project as regards financial, operational, legal and reputational risks.
184. Special attention should be paid to the outsourcing of critical activities in respect of which the occurrence of a problem may have a significant impact on the institution's ability to meet the regulatory requirements or even to continue its activities.
185. Special attention should be paid to the concentration and dependence risks which may arise when large parts of activities or important functions are outsourced to a single provider during a sustained period.
186. The institutions shall take into account the risks associated with the outsourcing "chains" (where a service provider outsources part of his/her 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.
187. The outsourcing policy should consider the impact of outsourcing on the institution's business and the risks it faces. It shall include reporting requirements

to which the service providers and 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 challenge the CSSF's supervision.

188. Special attention should be paid to the continuity aspects and the revocable nature of outsourcing. The institution shall be able to continue to operate normally in case of exceptional events or crisis. In this respect, the outsourcing agreements shall not include termination clauses or service termination clauses because of reorganisation measures or a winding-up procedure applied to the institution, as provided for in Part IV of the LFS. The institution shall also take the necessary measures to be in a position to adequately transfer the outsourced activities to a different provider or to perform those activities itself whenever the continuity or quality of the service provision are likely to be affected.
189. For each outsourced activity, the institution shall designate from among its employees a person who will be in charge of managing the outsourcing relationship and managing access to confidential data.

#### **Section 7.4.2. Specific IT outsourcing requirements**

190. The institution shall implement an IT policy which covers all IT activities scattered among the institution and its subcontractor(s). The IT organisation shall be adapted in order to integrate the outsourced activities to the proper functioning of the institution and the procedure manual shall be adapted accordingly. The institution's continuity plan shall be established in accordance with the continuity plan of its subcontractor(s).
191. The IT system security policy of the institution should consider the personal security established by its subcontractor(s) in order to ensure the overall consistency.
192. IT outsourcing may cover consulting, development and maintenance services (Sub-section 7.4.2.2), hosting services (Sub-section 7.4.2.3) or IT system management/operation services (Sub-section 7.4.2.1).

##### **Sub-section 7.4.2.1. IT system management/operation services**

193. The institutions may contractually use services for the management/operation of their systems:
  - In Luxembourg, solely from:
    - a credit institution or a financial professional holding a support PFS authorisation in accordance with Articles 29-3 and 29-4 of the LFS (primary IT systems operators of the financial sector or secondary IT systems and communication networks operators of the financial sector);
    - an entity of the group to which the institution belongs and which exclusively deals with group transactions provided that these systems do not include any readable confidential data on the customers other than institutional customers, unless explicit consent is given by the customer or the owner of the data or his/her proxy, on the basis of an informed opinion on the purpose of this outsourcing, the specific nature of the final goal, of the content of the provided information, of the recipient and

location as well as of the sustainability; in respect of institutional customers, the specific characteristics of this outsourcing shall be made explicit in the agreement.

- Abroad, from:
  - an entity of the group to which the institution belongs provided that these systems do not include any readable confidential data on customers other than institutional customers, unless explicit consent is given by the customer or the owner of the data or his/her proxy, on the basis of an informed opinion on the purpose of this outsourcing, the specific nature of the final goal, of the content of the provided information, of the recipient and location as well as of the sustainability; in respect of institutional customers, the specific characteristics of this outsourcing shall be made explicit in the agreement.

#### **Sub-section 7.4.2.2. Consulting, development and maintenance services**

194. The consulting, development and maintenance services may be contracted with any IT service provider, including an IT service of the group to which the institution belongs or a support PFS.
195. Prohibition to access confidential data shall also be applicable to third-party subcontractors other than support PFS which provide consulting, development or maintenance services. These third parties shall operate by default outside the IT 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 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.
196. Any change in the application functionality by a third party - other than the changes relating to corrective maintenance - shall be submitted for approval to the institution prior to its implementation.
197. The institution shall ensure that there are, if needed, no legal obstacles to obtain access to 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, for a period compatible with a transfer of this outsourcing to another subcontractor or a taking over of the applications concerned by the institution itself.

#### **Sub-section 7.4.2.3. Hosting services and infrastructure ownership**

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

Where the IT infrastructure includes confidential data, only the staff of the support PFS 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) of the LFS and is the subject of a service contract enabling this autonomy. Where the subcontractor is not a PFS, it cannot

intervene on the premises 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 of the institution is required for each intervention on the IT infrastructure, except interventions carried out by a support PFS as part of its mandate.

199. It is not mandatory for the processing centre to be physically located in the premises of the entity which is contractually responsible for the management of the IT systems. Whether the processing centre is in Luxembourg or abroad, it is thus possible that the hosting of the site is entrusted with another provider than that which provides IT system management services. In this case, the institution shall ensure that the principles contained in this sub-chapter are complied with by the entity which is contractually responsible for the management of IT systems and that the sub-outsourcing process is under control.
200. Where the processing centre is in Luxembourg, it may be hosted at a provider other than a credit institution or a support PFS, provided that it has no physical and logical access to the institution's systems.
201. Where the processing centre is abroad, no confidential data which enables the identification of a customer of the institution can be stored therein, unless it is encrypted and provided that the decryption can only be carried out within the institution or a support PFS within the context of its service provision or if all customers of the institution fulfil the conditions of express and informed consent as defined in point 193.

### **Section 7.4.3. Additional general requirements**

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

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

203. In case of IT service provision via telecommunication, the institution shall ensure that:
  - sufficient safeguards are taken in order to avoid that non-authorised persons access its system. The institution shall, in particular, make sure that telecommunications are encrypted or protected through other available technical resources likely to ensure the security of communication;
  - the IT link enables the Luxembourg institution to have quick and unfettered access to the information stored in the processing unit (i.e. through an adapted access path and debit and through data recovery).
204. The institution shall ensure that the capture, printing, backup, storage and archiving mechanisms guarantee confidentiality of data.
205. Outsourcing shall 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

allow keeping regular accounts in accordance with the rules applicable in Luxembourg and thus respecting the form and content rules imposed by the Luxembourg accounting laws and regulations.

206. 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**

207. Any outsourcing of 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. Any outsourcing approval shall be the subject of an official and detailed contract (including specifications).
208. The written documentation should 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.
209. 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 to exercise their controls.

### **Chapter 8. Legal reporting**

210. Credit institutions shall provide the CSSF with the ICAAP report and compliance certificate 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 month of the general meeting having approved the annual accounts. The relevant information are to 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. Risk management**

211. The risks shall be assessed based on an objective and critical analysis specific to the institution. It should not exclusively rely on external assessments.
212. 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.

213. The risk policy shall describe how the various risks are identified, measured, reported, managed, limited and controlled. 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 that the institution has a thorough overview of all the risks at all times.
214. The institutions shall have an internal limit and alert threshold system in respect of all their risks.
215. The risks toward related parties are to be dealt with internally as risks toward third parties. The internal governance arrangements shall apply to them in their entirety.

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

216. The risk measurement and reporting arrangements should 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.
217. The decisions on risk-taking and strategies and risk policies should 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.
218. In general, the risk measurement techniques implemented by an institution should be based on choices, assumptions and approximations. There is no absolute measurement.

Consequently, the institutions shall avoid any excess of confidence in any specific methodology or model. The risk measurement techniques used shall 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.

### **Chapter 2. Concentration risk**

219. Concentration risk results, in particular, from large (concentrated) exposures to customers or counterparties, respectively, or groups of customers or related counterparties, including related parties, on countries or sectors (industries) as well as on specific products or markets (intra-risk concentration). These exposures may be assets and liabilities 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 or systemic risk) which combine (inter-risk concentration).

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

220. Points 211 to 215 shall apply, in particular, to concentration risk.

## **Chapter 3. Credit risk**

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

221. Each credit risk-taking shall be subject to a written analysis which should cover at least the debtor's creditworthiness, the repayment plan 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.

222. Each credit risk-taking shall be subject to a predetermined decision-making process which should also involve a body separate from the business function.
223. 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.

224. 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.
225. 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.

226. 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 unlikelihood to pay.

227. 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 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.

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.

228. 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.

229. 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**

230. 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. Risk transfer pricing**

231. The institution 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 and the principle of sound and prudent business management.

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

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

## **Chapter 5. Private wealth management (“private banking”)**

234. The institutions shall have sound arrangements to ensure that the business relationships with their customers comply with the contracts entered into with these customers. This objective may be best achieved when the discretionary management, advice management and simple execution activities are separated from an organisational point of view.
235. The institutions shall have sound arrangements to ensure compliance with the customers’ risk profiles, for the purpose in particular of fulfilling the requirements arising from the MiFID regulations.
236. The institutions shall have sound arrangements 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 be separated from the business function.
237. Transfers and withdrawals of valuables (for instance cash and bearer instruments) shall be carried out and controlled by a function separated from the business function.
238. Any amendment of customers' identification data shall be carried out and controlled by an independent function from the business function.
239. If a customer purchases an exchange-traded derivative, the institution shall forthwith pass on (at least) the margin calls to be provided by the institution to the customer.
240. The institutions shall have sound arrangements in respect of credit and bank overdraft within the context of the private banking activities. The financial guarantees covering these credits shall be sufficiently diversified and liquid. For the purpose of having an adequate security margin, prudent discounts shall be applied according to the nature of the financial collateral. The institutions shall have an early warning system independent from the business function which should organise the monitoring of the financial collateral’s value and trigger the liquidation process of the financial guarantees. It shall ensure that the liquidation process is triggered in good time, and in any case before the value of the collateral becomes lower than the credit. Contracts with customers shall clearly describe the procedure triggered in the event of inadequacy of the guarantees.

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

241. 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.

242. Circulars IML 93/94 and CSSF 10/466 shall be repealed as from 1 July 2013.
243. 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.

244. 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 [www.eba.europa.eu](http://www.eba.europa.eu) and ESMA's website ([www.esma.europa.eu](http://www.esma.europa.eu)).

COMMISSION DE SURVEILLANCE DU SECTEUR FINANCIER

Claude SIMON	Andrée BILLON	Simone DEL COURT	Jean GUILL
Director	Director	Director	Director General