

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

Luxembourg, 22 December 2016

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

CIRCULAR CSSF 16/647

Re: Update of Circular CSSF 12/552 on the central administration, internal governance and risk management following the adoption of the European Banking Authority (EBA) guidelines relating to the limits on exposures to shadow banking entities which carry out banking activities outside a regulated framework under Article 395(2) of Regulation (EU) No 575/2013 (EBA/GL/2015/20)

Ladies and Gentlemen,

The purpose of this circular is to draw your attention to the guidelines of the European Banking Authority (EBA) relating to the limits on exposures to shadow banking entities which carry out banking activities outside a regulated framework under Article 395(2) of Regulation EU No 575/2013¹ (hereafter “shadow banking entities”) (EBA/GL/2015/20)² which will enter into force on 1 January 2017 and which the CSSF has committed itself to comply with in its capacity as competent authority.

EBA/GL/2015/20 shall apply to all institutions to which Part Four (“Large exposures”) of Regulation (EU) No 575/2013 (the “CRR”) applies, in accordance with the level of application set out in Part One, Title II of the CRR.

These guidelines define the concept of “shadow banking entity” and specify the principles to be complied with by the institutions when managing and measuring credit, individual or concentration risks which may arise from exposures to shadow banking entities. To this end, the guidelines specify the internal control mechanisms on which the institutions shall base their risk management. In addition, the guidelines specify how exposures to shadow banking entities should be treated in the context of the regulations on the limits to large exposures of the CRR.

¹ Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012.

² The guidelines are available at: <https://www.eba.europa.eu/regulation-and-policy/large-exposures/guidelines-on-limits-on-exposures-to-shadow-banking>.

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

Shadow banking entities referred to in the EBA guidelines are notably:

- any undertaking that invests in financial assets with a residual maturity not exceeding two years (short-term assets) and that have as distinct or cumulative objectives offering returns in line with money market rates or preserving the value of the investment (money market funds);
- alternative investment funds entitled to grant loans and/or undertakings employing leverage on a substantial basis;³
- undertakings carrying out at least the activities referred to in points 1 to 3, 6 to 8 and 10 of Annexe 1 of Directive 2013/36/EU.

This circular amends the points of Circular CSSF 12/552 relating to risk management. In order to facilitate the reading and the understanding, the amendments are presented in track changes (Annex 1).

EBA/GL/2015/20 shall enter into force on 1 January 2017. The institutions are required to update their internal processes and procedures in order to comply with all the provisions of the guidelines as from this date. For sake of completeness, a full copy of the guidelines are attached to this circular (Annex 2).

Yours faithfully,

COMMISSION DE SURVEILLANCE DU SECTEUR FINANCIER

Jean-Pierre FABER
Director

Françoise KAUTHEN
Director

Claude SIMON
Director

Simone DELCOURT
Director

Claude MARX
Director General

Annex 1

Annex 2

³ In accordance with Article 111(1) of Commission Delegated Regulation (EU) No 231/2013 of 19 December 2012 supplementing Directive 2011/61/EU of the European Parliament and of the Council with regard to exemptions, general operating conditions, depositaries, leverage, transparency and supervision.

COMMISSION de SURVEILLANCE du SECTEUR FINANCIER

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 performing lending operations¹

CIRCULAR CSSF 12/552 as amended by Circulars CSSF 13/563, CSSF 14/597, CSSF 16/642 and CSSF 16/647

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 10/466².

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

² 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.³

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

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

The same applies to risk. This circular essentially transposes the [CEBS guidelines and the EBA guidelines dated 2 September 2010 on concentration risk \("CEBS Guidelines on the management of concentration risk under the supervisory review process \(GL31\)"\), the guidelines dated 27 October 2010 on liquidity pricing \("Guidelines on Liquidity Cost Benefit Allocation"\), the EBA guidelines of 22 May 2015 on the management of interest rate risk arising from non-trading activities \(EBA/GL/2015/08\) and the EBA guidelines of 14 December 2015 relating to the limits on exposures to shadow banking entities which carry out banking activities outside a regulated framework under Article 395\(2\) of Regulation \(EU\) No 575/2013 \(EBA/GL/2015/20\)](#). Moreover, the circular highlights the basic principles of prudence in the field of credit granting and private wealth management.

[As far as CRR institutions⁴ are concerned, this circular shall be read in conjunction with CSSF Regulation N° 15-02 relating to the supervisory review and evaluation process that applies to CRR institutions.](#)

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

³ 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.

⁴ [The term "CRR institution" is defined in Article 1\(1\) of CSSF Regulation N° 15-02.](#)

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.

Table of contents

Part I.	Definitions and scope	6
Chapter 1.	Definitions	6
Chapter 2.	Scope	6
Part II.	Central administration and internal governance arrangements	8
Chapter 1.	Central administration	8
Chapter 2.	Internal governance arrangements.....	8
Chapter 3.	General characteristics of "robust" central administration and internal governance arrangements.....	10
Chapter 4.	Board of directors and authorised management	11
Sub-chapter 4.1.	Board of directors.....	11
Section 4.1.1.	Responsibilities of the board of directors	11
Section 4.1.2.	Composition and qualification of the board of directors	15
Section 4.1.3.	Organisation and functioning of the board of directors.....	15
Section 4.1.4.	Specialised committees	16
Sub-section 4.1.4.1.	Audit committee	17
Sub-section 4.1.4.2.	Risk committee.....	18
Sub-chapter 4.2.	Authorised management.....	19
Section 4.2.1.	Responsibilities of the authorised management	19
Section 4.2.2.	Qualification of the authorised management.....	22
Section 4.2.3.	Specific (risk, capital and liquidity) policies	22
Chapter 5.	Administrative, accounting and IT organisation	23
Sub-chapter 5.1.	Organisation chart and human resources.....	23
Sub-chapter 5.2.	Administrative and technical infrastructure	24
Section 5.2.1.	Administrative infrastructure of the business functions	24
Section 5.2.2.	Financial and accounting function.....	24
Section 5.2.3.	IT function.....	26
Section 5.2.4.	Internal communication and whistleblower arrangements	27
Section 5.2.5.	Crisis management arrangements.....	27
Sub-chapter 5.3.	Internal documentation.....	27
Chapter 6.	Internal control	28
Sub-chapter 6.1.	Operational controls	29
Section 6.1.1.	Day-to-day controls carried out by the operating staff.....	29
Section 6.1.2.	Ongoing critical controls	29
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	30
Sub-chapter 6.2.	Internal control functions	30
Section 6.2.1.	General responsibilities of the internal control functions.....	31
Section 6.2.2.	Characteristics of the internal control functions.....	31
Section 6.2.3.	Execution of the internal control functions' work.....	33
Section 6.2.4.	Organisation of the internal control functions	34
Section 6.2.5.	Risk control function	35
Sub-section 6.2.5.1.	Specific responsibilities and scope of the risk control function	36
Sub-section 6.2.5.2.	Organisation of the risk control function.....	36
Section 6.2.6.	Compliance function	37
Sub-section 6.2.6.1.	Compliance charter.....	37
Sub-section 6.2.6.2.	Specific responsibilities and scope of the compliance function	38
Sub-section 6.2.6.3.	Organisation of the compliance function.....	40
Section 6.2.7.	Internal audit function	41
Sub-section 6.2.7.1.	Internal audit charter	41
Sub-section 6.2.7.2.	Specific responsibilities and scope of the internal audit function ..	42

Sub-section 6.2.7.3.	Execution of the internal audit work	43
Sub-section 6.2.7.4.	Organisation of the internal audit function.....	44
Chapter 7.	Specific requirements	45
Sub-chapter 7.1.	Organisational structure and legal entities (Know-your-structure)	45
Section 7.1.1.	Guiding principles as regards "non-standard" or "non-transparent" activities.....	46
Sub-chapter 7.2.	Management of conflicts of interest.....	46
Section 7.2.1.	Additional requirements relating to the conflicts of interest involving related parties	47
Sub-chapter 7.3.	New Product Approval Process.....	48
Sub-chapter 7.4.	Outsourcing	48
Section 7.4.1.	General outsourcing requirements.....	49
Section 7.4.2.	Specific IT outsourcing requirements	50
Sub-section 7.4.2.1.	IT system management/operation services.....	51
Sub-section 7.4.2.2.	Consulting, development and maintenance services	51
Sub-section 7.4.2.3.	Hosting services and infrastructure ownership.....	52
Section 7.4.3.	Additional general requirements	53
Section 7.4.4.	Documentation	53
Chapter 8.	Legal reporting	54
Part III.	Risk management	54
Chapter 1.	General principles as regards risk measurement and risk management.....	54
Sub-chapter 1.1.	Risk management	54
Sub-chapter 1.2.	Risk measurement	54
Chapter 2.	Concentration risk	55
Chapter 3.	Credit risk.....	55
Sub-chapter 3.1.	General principles.....	55
Sub-chapter 3.2.	Residential mortgages to individuals.....	57
Sub-chapter 3.3.	Credit to real estate developers.....	58
Chapter 4.	Risk transfer pricing	58
Chapter 5.	Private wealth management (“private banking”).....	59
Chapter 6.	Exposures to shadow banking entities.....	59
Sub-chapter 6.1.	Implementation of sound internal control principles.....	59
Sub-chapter 6.2.	Application of quantitative limits.....	60
Chapter 7.	Asset encumbrance.....	61
Chapter 8.	Interest rate risk arising from non-trading book activities	62
Part IV.	Entry into force, transitional measures and repealing provisions...	62

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);
 - 5) "LFS" shall mean the law of 5 April 1993 on the financial sector;
 - 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.

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

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

Chapter 6 of Part III of this circular applies only to credit 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 as well as the procedures governing the composition, responsibilities, organisation and operation of the board of directors.⁵ 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 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).

⁵ 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 other⁶ - 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.

⁶ Including an employment relationship.

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.

Sub-section 4.1.4.1. Audit committee⁷

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, on⁸:
 - 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;

⁷ 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.

⁸ 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 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
 - 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 report⁹ 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.

⁹ Cf. point 26 of Circular CSSF 07/301.

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.

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 Chief Compliance Officer pursuant to point 141, cannot, at the same time, be in charge of 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.¹⁰
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;

¹⁰ 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.

- 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 Subchapter 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*:

- 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 in compliance with the

prudential authorisation procedure of key function holders as published by the CSSF on its website.

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

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

Section 6.2.1. General responsibilities of the internal control functions

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

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

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 their significance and 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

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 standards¹¹;
- 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;

¹¹ 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.¹²
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

¹² 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."

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.
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. A notification to the CSSF stating that the conditions laid down in this circular are complied with is sufficient where the institution resorts to a Luxembourg credit institution or a support PFS in accordance with Articles 29-1, 29-2, 29-3 and 29-4 of the LFS;
- The access of the CSSF, the *réviseur d'entreprises agréé* and the internal control functions of the institution to the information relating to the outsourced activities shall 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 LTV, 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.

Chapter 6. Exposures to shadow banking entities

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

Sub-chapter 6.1. Implementation of sound internal control principles

242. The institutions shall put in place an internal framework for the identification, management, control and mitigation of the risks arising from the exposures to shadow banking entities¹³ in accordance with EBA/GL/2015/20.

¹³ Shadow banking entities are defined in paragraph 11 “Definitions” of EBA/GL/2015/20. These entities are undertakings that carry out one or more credit intermediation activities and that are not excluded undertakings within the meaning of said paragraph. “Credit intermediation activities” shall

243. The institutions shall apply a materiality threshold to identify the exposures to shadow banking entities. In accordance with EBA/GL/2015/20, any individual exposure to shadow banking entity that is equal or in excess of 0.25%¹⁴ of the institution's eligible capital¹⁵ after taking into account the effect of the credit risk mitigation and exemptions¹⁶, shall be taken into consideration and cannot be deemed as low exposure.

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

Sub-chapter 6.2. Application of quantitative limits

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

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

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

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

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

249. When setting those limits, as part of their internal assessment process, the institutions should take into account:

- the regulatory status of the shadow banking entity, in particular whether it is subject to any type of prudential or supervisory requirements;
- the financial situation of the shadow banking entity including, but not limited to, its capital position, leverage and liquidity position;
- information available about the portfolio of the shadow banking entity, in particular non-performing loans;

mean: "bank-like activities involving maturity transformation, liquidity transformation, leverage, credit risk transfer or similar activities".

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

¹⁵ Within the meaning of point (71) of Article 4(1) of Regulation (EU) No 575/2013.

¹⁶ i) Credit risk mitigating effects in accordance with Articles 399 and 403 of Regulation (EU) No 575/2013;

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

- available evidence about the adequacy of the credit analysis performed by the shadow banking entity on its portfolio, if applicable;
 - whether the shadow banking entity will be vulnerable to asset price or credit quality volatility;
 - concentration of credit intermediation activities relative to other business activities of the shadow banking entity;
 - interconnectedness between, on the one hand, shadow banking entities and, on the other hand, between shadow banking entities and the institution;
 - any other relevant factors identified by the institution as exposures to shadow banking entities, all potential risks to the institution arising from those exposures, and the potential impact of those risks.
250. If institutions are not able to apply the principal approach as set out above, their aggregate exposures to shadow banking entities should be subject to the limits on large exposures in accordance with Article 395 of Regulation (EU) No 575/2013 (hereinafter the “fallback approach”).
251. The fallback approach should be applied in the following way:
- If institutions cannot meet the requirements regarding effective processes and control mechanisms or oversight by their management body as set out in Section 4 of EBA/GL/2015/20, they should apply the fallback approach to all their exposures to shadow banking entities (i.e. the sum of all their exposures to shadow banking entities).
 - If institutions can meet the requirements regarding effective processes and control mechanisms or oversight by their management body as set out in Sub-chapter 6.1, but cannot gather sufficient information to enable them to set out appropriate limits as set out in Section 6.2.1, they should only apply the fallback approach to the exposures to shadow banking entities for which the institutions are not able to gather sufficient information. The principal approach as set out in Section 6.2.1 should be applied to the remaining exposures to shadow banking entities.

Chapter 7. Asset encumbrance

241-252. This chapter only applies to credit institutions.

242-253. The credit institutions shall put in place risk management policies to define their approach to asset encumbrance as well as procedures and controls that ensure that the risks associated with collateral management and asset encumbrance are adequately identified, monitored and managed. These policies should take into account each credit institution’s business model, the Member States in which they operate, the specificities of the funding markets and the macroeconomic situation. The policies should be approved in accordance with the provisions of point 19.

243-254. The credit institutions shall have in place a general monitoring framework that provides timely information, at least once a year, to the authorised management and the board of directors on:

- the level, evolution and types of asset encumbrance and related sources of encumbrance, such as secured funding or other transactions;

- the amount, evolution and credit quality of unencumbered but encumberable assets, specifying the volume of assets available for encumbrance;
- the amount, evolution and types of additional encumbrance resulting from stress scenarios (contingent encumbrance).

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

Specification:

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

Chapter 8. Interest rate risk arising from non-trading book activities

245.256. CRR institutions¹⁷, when implementing Article 14 (Interest risk arising from non-trading book activities) of CSSF Regulation N° 15-02 relating to the supervisory review and evaluation process that applies to CRR institutions, shall comply with the guidelines published by the European Banking Authority in this respect.¹⁸ Investment firms which are not CRR investment firms do not fall within this chapter.

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

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

247.258. 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);

¹⁸ “Guidelines on the management of interest rate risk arising from non-trading activities” (EBA/GL/2015/08) available on the EBA’s website: <https://www.eba.europa.eu/-/eba-updates-guidelines-on-interest-rate-risk-arising-from-non-trading-activities>.

- The need to lay down in writing the guidelines provided for in indents 4 to 8 of point 17.

~~248.259.~~ Circulars IML 93/94 and CSSF 10/466 shall be repealed as from 1 July 2013.

~~249.260.~~ 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.

~~250.261.~~ 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) and ESMA’s website (www.esma.europa.eu).

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

The aforementioned recommendation is available on the ESRB’s website (www.esrb.europa.eu).

- Circular CSSF 16/642 implementing the EBA Guidelines on the management of interest rate risk arising from non-trading activities – EBA/GL/2015/08.

- Circular CSSF 16/647 implementing the EBA guidelines relating to the limits on exposures to shadow banking entities which carry out banking activities outside a regulated framework under Article 395(2) of Regulation (EU) No 575/2013 (EBA/GL/2015/20).

The above-mentioned guidelines are available on the EBA’s website (www.eba.europa.eu).

COMMISSION DE SURVEILLANCE DU SECTEUR FINANCIER

Claude SIMON

Director

Simone
DEL COURT

Director

Jean GUILL

Director General

EBA/GL/2015/20

14 December 2015

Guidelines

Limits on exposures to shadow banking entities which carry out banking activities outside a regulated framework under Article 395(2) of Regulation (EU) No 575/2013

Contents

1. Executive Summary	3
2. Background and rationale	5
3. Guidelines	16
4. Accompanying documents	30
4.1 Cost-Benefit Analysis/Impact Assessment	30
4.2 Views of the Banking Stakeholder Group (BSG)	37
4.3 Feedback on the public consultation and on the opinion of the BSG	41

1. Executive Summary

Under Article 395(2) of Regulation (EU) No 575/2013, the EBA has a mandate to develop guidelines to set appropriate aggregate limits or tighter individual limits on exposures to shadow banking entities which carry out banking activities outside a regulated framework.

The global financial crisis has revealed previously unrecognised fault lines which can transmit risk from the shadow banking system to the regulated banking system, putting the stability of the entire financial system at risk.

From a microprudential perspective, shadow banking entities are generally not subject to the same standards of prudential regulation as core regulated entities such as institutions, do not provide protection to investors' investment from these entities' failures, and do not have access to central banks' liquidity facilities. To the extent that shadow banking entities carry out bank-like activities, exposures to such entities may therefore be inherently risky - and thus specific limits for individual and aggregate exposures could be warranted.

Macro prudentially, institutions' exposures to shadow banking entities could be of concern for different reasons. Here, institutions' exposures to such entities undertaking bank-like activity may lead to regulatory arbitrage concerns, and worries that core banking activity may migrate systematically away from the regulated sector 'into the shadows'. In order to seek profits, institutions may still actively seek ways to arbitrage the rules by funding shadow banking entities. These entities, which are potentially more vulnerable to runs and/or liquidity problems, tend to be highly correlated and interconnected with the banking sector, which leads to financial stability concerns.

To minimise the risks posed to institutions arising from their exposures to shadow banking entities, the guidelines lay down requirements for institutions to set limits, as part of their internal processes, on their individual exposures to shadow banking entities (alleviating primarily the microprudential concerns expressed above) and on their aggregate exposure to shadow banking entities (alleviating macroprudential concerns).

In the absence of a definition in Regulation (EU) No 575/2013 of the terms 'shadow banking entities', 'banking activities' and 'regulated framework', it has been necessary to develop a definition of those terms for the purposes of the guidelines. The definitions proposed are in line with the previous EBA Opinion and Report on the perimeter of credit institutions¹ and aim at capturing entities that are not subject to appropriate prudential regulation and supervision, and therefore pose the greatest risks.

¹ The Opinion and Report are available here: <http://www.eba.europa.eu/-/eba-publishes-an-opinion-on-the-perimeter-of-credit-institutions>.

To better understand the relevance of institutions' exposures to shadow banking entities and the impact of potential limits, a data collection was conducted and the results published in a separate report. The scope of the data collection was, however, broader than the current scope of the guidelines so as to provide a sound basis for the calibration of any limits and to assist the European Commission's work in relation to its report on the appropriateness and impact of imposing limits on exposures to shadow banking entities under the last subparagraph of Article 395(2) of Regulation (EU) No 575/2013.

In prescribing the approach institutions should adopt for the purposes of setting appropriate individual and aggregate limits for exposures to shadow banking entities, these guidelines will establish a harmonised approach for mitigating the risks identified above and will also inform the European Commission's report.

Next steps

The guidelines will be translated into the official EU languages and published on the EBA website. The deadline for competent authorities to report on whether they comply with the guidelines will be two months after the publication of the translations. The guidelines will apply from 01/01/2017.

2. Background and rationale

2.1 General background

1. Shadow banking can complement traditional banking by expanding valuable access to credit in support of economic activity or by supporting market liquidity, maturity transformation and risk sharing, thereby supporting growth in the real economy. For example, various types of non-bank funds have stepped in (often as intermediaries for insurance companies and pension funds) to provide long-term credit to the private sector while banks have been repairing their balance sheets and retrenching from certain activities². Moreover, in the euro area, recent data shows that lending by shadow banks as a proportion of total lending is rising³. Research also suggests that shadow banking often enhances the efficiency of the financial sector by enabling better risk sharing and maturity transformation and by deepening market liquidity⁴.
2. However, the global financial crisis has revealed previously unrecognised fault lines in the shadow banking system which put the stability of the financial system at risk. These include a heavy reliance on short-term wholesale funding and a general lack of transparency, which masked the increasing amounts of leverage, maturity and liquidity transformation in the run-up to the crisis, and in turn increased the vulnerability of shadow banking entities to runs. The subsequent fire sale of assets by such entities helped spread the stress to the traditional banking system.
3. A number of international regulatory initiatives relating to shadow banking have been undertaken and some are currently in progress. For example, in April 2011 the Financial Stability Board (FSB) published Recommendations to Strengthen Oversight and Regulation of Shadow Banking⁵ and in April 2014 the Basel Committee on Banking Supervision (BCBS) published a revised supervisory framework for measuring and controlling large exposures, which includes exposures to shadow banking entities⁶. At the EU level, the Commission has adopted a proposal for a regulation aimed at increasing transparency of certain transactions outside the regulated banking sector⁷. Additionally, work has been undertaken to analyse the scope of the perimeter of credit

² See IMF Global Financial Stability Report, April 2014, available here: <http://www.imf.org/external/pubs/FT/GFSR/2014/01/index.htm>.

³ See IMF Global Financial Stability Report, October 2014, available here: <http://www.imf.org/external/pubs/ft/gfsr/2014/02/>; and the Financial Stability Board's Global Shadow Banking Monitoring Report 2014, available here: <http://www.financialstabilityboard.org/2014/11/global-shadow-banking-monitoring-report-2014/>.

⁴ Claessens, Stijn, Zoltan Pozsar, Lev Ratnovski and Manmohan Singh, December 2012, 'Shadow Banking: Economics and Policy', IMF Staff Discussion Note SDN/12/12, International Monetary Fund, Washington, DC.

⁵ The FSB's recommendations are available here: <http://www.financialstabilityboard.org/2011/10/financial-stability-board-publishes-recommendations-to-strengthen-oversight-and-regulation-of-shadow-banking/>.

⁶ 'Supervisory framework for measuring and controlling large exposures - final standard', Basel Committee on Banking Supervision, Bank for International Settlements, April 2014.

⁷ Proposal for a regulation of the European Parliament and of the Council on reporting and transparency of securities financing transactions, European Commission, January 2014.

institutions in the EU, the results of which are set out in the EBA's Opinion and Report on the perimeter of credit institutions⁸. At the international level, work led by the BCBS is under way on accounting and regulatory approaches to consolidation. The FSB is also conducting intensive monitoring of the shadow banking sector⁹ and investigating financial stability risks from asset management activities¹⁰.

2.1.1 Concerns regarding shadow banking entities

4. Whilst some activities carried out by shadow banking entities can have beneficial effects as regards the financing of the real economy and fostering growth, they also generate a number of specific risks from a prudential viewpoint that may warrant regulatory attention.
- *Run risk and/or liquidity problems:* Shadow banking entities are potentially vulnerable to runs (withdrawal of deposit-like assets due to panic, early redemptions due to a confidence crisis) and/or liquidity problems (liquidation of assets at fire sale prices), stemming from credit exposures, high leverage, and liquidity and maturity mismatches between assets and liabilities. These risks are usually exacerbated because shadow banking entities do not have sectoral liquidity backstops and are generally subject to less robust and comprehensive prudential standards and supervision.
 - *Interconnectivity and spillovers:* Shadow banking entities tend to be highly correlated and interconnected with the regulated banking sector due to ownership linkages and explicit and implicit credit commitments and as direct counterparties. In times of stress this can, directly or indirectly, generate systemic risks through contagion effects both between shadow banking entities and between such entities and the regulated banking sector, leading to a flight to quality and fire sales of assets.
 - *Excessive leverage and procyclicality:* The maturity mismatch and liquidity risks are exacerbated by shadow banking entities' ability to engage in highly leveraged or otherwise risky financial activities. Highly leveraged structures are more likely to become insolvent in the case of unexpected negative events due to inadequate loss-absorbing capacity, abrupt deleveraging and inability to roll over financing needs. The crystallisation of such events can trigger a confidence crisis in the regulated banking sector, leading to severe impairment of funding sources.
 - *Opacity and complexity:* The opaque and complex nature of governance and ownership structures of shadow banking entities and their relationships with the regulated banking sector constitute vulnerabilities, since, during periods of stress, investors tend to retrench and flee to safe, high-quality and liquid assets. The inherent agency problem, caused by the separation of financial intermediation activities across multiple shadow banking entities, also

⁸ The EBA's Opinion and Report are available here: <https://www.eba.europa.eu/-/eba-publishes-an-opinion-on-the-perimeter-of-credit-institutions>.

⁹ See for example the FSB's Global Shadow Banking Monitoring Report 2014 as referred to in footnote 2.

¹⁰ <http://www.financialstabilityboard.org/2015/07/next-steps-on-the-nbni-g-sifi-assessment-methodologies/>

contributes to vulnerabilities in the financial system. Furthermore, there is a lack of disclosure (regarding collateral, assets or value thereof), as such entities are generally unregulated or subject to less robust prudential regulation.

2.1.2 Legal mandate and definitions used

5. The EBA has the mandate under Regulation (EU) No 575/2013¹¹ to issue guidelines to set limits on institutions' exposures to shadow banking entities.

6. Article 395(2) of Regulation (EU) No 575/2013 reads as follows:

'EBA shall, in accordance with Article 16 of Regulation (EU) No 1093/2010, taking into account the effect of the credit risk mitigation in accordance with Articles 399 to 403 as well as the outcomes of developments in the area of shadow banking and large exposures at the Union and international levels, issue guidelines by 31 December 2014 to set appropriate aggregate limits to such exposures or tighter individual limits on exposures to shadow banking entities which carry out banking activities outside a regulated framework.'

'In developing those guidelines, EBA shall consider whether the introduction of additional limits would have a material detrimental impact on the risk profile of institutions established in the Union, on the provision of credit to the real economy or on the stability and orderly functioning of financial markets.'

7. In the absence of a definition in Regulation (EU) No 575/2013 of the terms 'shadow banking entities', 'banking activities' and 'regulated framework', for the purposes of these guidelines, the EBA defines shadow banking entities as entities that:

- a. carry out credit intermediation activities, defined as bank-like activities involving maturity transformation, liquidity transformation, leverage, credit risk transfer or similar activities; and
- b. are neither within the scope of prudential consolidation nor subject to solo prudential requirements under specified EU legislation (or equivalent third country legal frameworks). Entities referred to in Article 2(5) and Article 9(2) of Directive 2013/36/EU¹², as well as other entities as defined in the guidelines ('excluded undertakings'), are also not to be regarded as shadow banking entities.

8. This approach is consistent with the EBA's Opinion and Report on the perimeter of credit institutions¹³. In particular, the guidelines do not prescribe an exhaustive list of activities that fall within the scope of credit intermediation activities. Instead, the description of 'credit

¹¹ Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 321, 30.11.2013, p. 6).

¹² Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

¹³ See footnote 8.

intermediation' adopted in the aforementioned Opinion and Report, which follows the approach prescribed by the FSB, has been adopted, as this best describes the types of activities undertaken by shadow banking entities. The FSB has identified the four key features of credit intermediation as: (a) maturity transformation (borrowing short and lending/investing on longer timescales); (b) liquidity transformation (using cash-like liabilities to buy less liquid assets); (c) leverage; and (d) credit risk transfer (transferring the risk of credit default to another person for a fee). Examples of entities carrying out credit intermediation include money market funds (MMFs), special-purpose vehicles (SPVs) engaged in securitisation transactions, securities and derivatives dealers, and companies engaged in factoring, leasing or hire purchase.

9. In order to assist institutions in identifying entities that are carrying out credit intermediation activities, the guidelines make it clear that entities carrying out one or more of the activities listed in the following points of Annex 1 of Directive 2013/36/EU shall be automatically regarded as carrying out credit intermediation activities: points 1 (taking deposits and other repayable funds), 2 (lending), 3 (financial leasing), 6 (guarantees and commitments), 7 (trading for own account or for account of customers in specified forms of financial instrument), 8 (participation in securities issues and the provision of services relating to such issues) and 10 (money broking). However, this should not be taken as an exhaustive list of activities within the scope of 'credit intermediation'. Rather, this approach simply confirms specific cases in which entities are to be positively identified as carrying out credit intermediation activities for the purposes of the guidelines.
10. The second limb of the definition of shadow banking entities for the purposes of the guidelines carves out certain entities from the scope of the definition (and therefore from the scope of the guidelines). These are entities that are subject to an appropriate and sufficiently robust prudential framework. For example, under this approach, credit institutions, investment firms, insurers and entities established in third countries which are subject to prudential requirements which are considered to be equivalent to those applied in the Union are out of the scope of the guidelines. Furthermore, entities subject to consolidated prudential supervision (whether as a result of EU legislation, applicable national legislation or an equivalent third country legal framework) are out of the scope of the guidelines.
11. Given this, the guidelines focus on institutions' exposures to entities that pose the greatest risks in terms of both the direct exposures institutions face and also the risk of credit intermediation being carried out outside the regulated framework (see further below). These entities include unregulated financial sector entities such as special-purpose entities (SPEs) and SPVs not covered by consolidated prudential supervision.
12. As regards funds, these tend to engage in maturity and liquidity transformation and are generally regarded as outside the traditional banking sector¹⁴. Therefore, *prima facie*, they should be within the scope of the definition of shadow banking entity.

¹⁴ For example, see the FSB's Global Shadow Banking Monitoring Report 2014.

13. However, some funds are regulated pursuant to prudential frameworks similar to those applied to credit institutions and investment firms. In particular, in the EU the UCITS (Undertakings for Collective Investments in Transferable Securities) Directive (Directive 2009/65/EC) prescribes a robust set of requirements under which undertakings for collective investment in transferable securities, and their managers, operate. These include requirements on the asset manager (initial capital, own funds and internal control requirements) and the managed funds (e.g. limits to leverage and concentration). Therefore, such funds do not pose the same level of risk to institutions in terms of credit and step-in/bail-out risk (e.g. due to reputational, franchise and other risks) as unregulated funds.
14. Notwithstanding these requirements, it is proposed that all MMFs, regardless of whether they operate under the rules of Directive 2009/65/EC or others, should be within the scope of the definition of shadow banking entity for the purposes of these guidelines. This is because, as acknowledged by the European Commission in its proposal for a regulation on MMFs¹⁵ (under negotiation), the average size of an MMF far exceeds the average size of a UCITS fund and, as acknowledged by the FSB and other institutions such as the International Organisation of Securities Commissions and the European Systemic Risk Board¹⁶, the systemic risks posed by such funds (in particular having regard to their interconnectedness with the banking sector) have not been addressed to an adequate degree through existing regulatory measures. Therefore, at this stage (in particular, pending agreement on the Commission's legislative proposal) the EBA includes all MMFs within the scope of the definition of shadow banking entity.
15. Regarding the treatment of alternative investment funds (AIFs), the EBA has considered the feedback received during the consultation period as well as input from the European Securities Market Authority (ESMA) and the European Commission. The EBA acknowledges that AIFs are regulated indirectly, as a result of requirements imposed on their asset managers under Directive 2011/61/EU (the AIFMD), e.g. initial capital, own funds and internal controls requirements. However, the risks arising directly from the funds themselves are not mitigated in a satisfactory way from a prudential point of view. For example, leverage is strictly limited for UCITS funds: they can borrow only up to 10% of their assets provided that such borrowing takes place on a temporary basis¹⁷. However, similar leverage limitation does not apply to AIFs, although they

¹⁵ The Commission's proposal is available here: http://ec.europa.eu/finance/investment/money-market-funds/index_en.htm.

¹⁶ IOSCO's recommendations are available here: <http://www.iosco.org/news/pdf/IOSCONEWS255.pdf>.

The ESRB's recommendations are available here: https://www.esrb.europa.eu/pub/pdf/recommendations/2012/ESRB_2012_1.en.pdf?c9daf560cb3d72433ca237604eda38af.

¹⁷ In most cases leverage is measured as a ratio between the fund exposure and its Net asset Value (NaV). Most UCITS are required to use the commitment approach, under which derivatives exposures are converted into equivalent cash positions. When UCITS engage in complex investment strategies or when the commitment approach does not adequately capture the market risk of their portfolio, they should use either the absolute or the relative Value at Risk (VaR). All AIFs are required to measure their exposure through the commitment method, similarly to UCITS. Under the commitment approach, UCITS exposure relating to derivative instruments cannot exceed the total net value of the portfolio. Eventually a UCITS using both external borrowing and derivatives can thus leverage up to 1.1 times its NaV (i.e. overall leverage of 2.1). For more sophisticated UCITS, the relative VaR approach does not measure the leverage of the strategies; rather it allows UCITS to double the risk of loss compared with a similar but unleveraged portfolio. Finally the VaR of a UCITS using the

must put in place risk management policies and are subject to stress testing and reporting obligations¹⁸. Given this, the EBA is of the view that only AIFs with limited leverage could be considered to fall outside the definition of ‘shadow banking entities’. Article 111(1) of Delegated Regulation 231/2013 considers leverage to be employed on a substantial basis when the AIF exposure exceeds 300% of its net asset value. Furthermore, only AIFs which are not entitled to grant loans or purchase third parties’ lending exposures onto their balance sheet should be excluded from the definition of ‘shadow banking entities’ for the purposes of these guidelines. On the contrary, AIFs which are entitled to grant loans carry out a typical banking activity outside the regulated banking system (i.e. Regulation (EU) No 575/2013 and Directive 2013/36/EU or comparable prudential regulation). These funds should therefore fall within the scope of the guidelines, as they act as substitutes for bank lending and could generate credit intermediation risks (i.e. runs and/or liquidity risk) without having a banking (or comparable) licence and they are not subject to harmonised rules on concentration risks, credit assessment, provisioning, etc.

16. Given this, all funds would be considered to fall within the scope of the definition of shadow banking entities except if they are non-MMF UCITS, AIFs meeting the criteria mentioned in the paragraph above or third country funds subject to requirements equivalent to the UCITS Directive.

17. Regarding the particular case of European Venture Capital Funds (EuVECAs), European Social Entrepreneurship Funds (EuSEFs) and European Long-Term Investment Funds (ELTIFs), the EBA is of the view that these funds should fall outside the definition of ‘shadow banking entity’ due to their type of activity, and should therefore be excluded from the scope of the guidelines.

18. This approach is consistent with the approach described in the EBA’s Opinion and Report on the perimeter of credit institutions¹⁹ and the general focus of the policy debate on shadow banking within the European Union and in international contexts²⁰.

2.1.3 Relation to other parts of the European rulebook

19. The guidelines should be applied independently from and in addition to the general large exposures framework as defined in Part Four of Regulation (EU) No 575/2013.

20. On 27 November 2014, Commission Delegated Regulation (EU) No 1187/2014 of 2 October 2014 supplementing Regulation (EU) No 575/2013 of the European Parliament and of the Council as regards regulatory technical standards for determining the overall exposure to a client or a group

absolute VaR approach cannot be greater than 20% of its NaV. The VaR approaches potentially allow higher leverage than the commitment approach, depending on the volatility of the underlying assets.

¹⁸ For an overview of leverage measures and restrictions, see ECB (2015), ‘[Financial Stability Review, Box 7: Synthetic leverage in the investment fund sector](#)’, May 2015, pp. 92-94.

¹⁹ See footnote 8.

²⁰ For example, see the Commission’s (2013) Communication on shadow banking: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013DC0614&from=EN>; the IMF’s 2014 Global Financial Stability Report: <http://www.imf.org/external/pubs/ft/gfsr/2014/02/>, which includes in Chapter 2 an assessment of the size and riskiness of shadow banking around the globe; and the Financial Stability Board’s 2014 Global Shadow Banking Monitoring Report, available here: <http://www.financialstabilityboard.org/2014/11/global-shadow-banking-monitoring-report-2014/>.

of connected clients in respect of transactions with underlying assets entered into force. This regulation applies to all exposures through transactions with underlying assets, thus also including exposures that are within the scope of the guidelines.

21. In addition, the EBA is updating the guidelines on the identification of groups of connected clients under Article 4(1)(39) of Regulation (EU) No 575/2013, including providing greater clarity on how institutions and shadow banking entities can be economically interdependent.

22. The guidelines should be read in conjunction with supervisory powers under the Supervisory Review and Evaluation Process (SREP) of Pillar 2. The articulation between these guidelines and Pillar 2 is further developed in the following section.

23. Finally, the guidelines are developed having regard to the Commission's mandate under Article 395 of Regulation (EU) No 575/2013 to 'assess the appropriateness and the impact of imposing limits on exposures to shadow banking entities which carry out banking activities outside a regulated framework' by 31 December 2015.

24. In developing the guidelines, the EBA is also mindful of other European and international workstreams in the area of shadow banking and large exposures. These include:

- An assessment by the European Commission of the current scope of application of the EU banking prudential rules, as part of the Commission's broader workstream on shadow banking²¹. The EBA provided an opinion on this matter, at the request of the Commission, in November 2014²².
- Work by the BCBS, on the scope of consolidation for prudential regulatory purposes to ensure all banks' activities are appropriately captured in prudential regimes. A public consultation on the proposals is expected by the end of 2015.
- A peer review, to be launched by the FSB in 2015, regarding its member jurisdictions' implementation of the FSB's policy framework for shadow banks, as well as the results of the FSB's fifth shadow banking monitoring exercise in late 2015²³.

2.1.4 Rationale for limiting institutions' exposures to shadow banking entities

25. Potential risks could arise from institutions' exposures to shadow banking entities from both a microprudential and a macroprudential perspective.

26. A general concern is that institutions' exposures to shadow banking entities undertaking bank-like activity may also lead to regulatory arbitrage concerns, and worries that core banking activity may migrate systematically away from the regulated sector 'into the shadows'. A range of regulations are now in place to address some of the arbitrage risks relating to shadow banking entities that

²¹ [Shadow Banking – Addressing New Sources of Risk in the Financial Sector](#), European Commission, 4 November 2013.

²² [Opinion of the European Banking Authority on Matters Relating to the Perimeter of Credit Institutions](#), EBA/Op/2014/12, 27 November 2014.

²³ [Updated G20 Roadmap towards Strengthened Oversight and Regulation of Shadow Banking in 2015](#), G20.

were observed during the financial crisis. For example, the risk weights on various forms of shadow banking exposures have increased. Nonetheless, as the regulatory regime for institutions tightens, the pressure for bank-like activity to be carried out elsewhere in the financial system increases.

27. From a microprudential perspective, banking activities such as maturity and liquidity transformation are inherently risky. For this reason, institutions are subject to robust prudential regulation, must participate in Deposit Guarantee Schemes and generally have access to central bank liquidity facilities. Shadow banking entities are generally unregulated or not subject to the same standards of prudential regulation as core regulated entities such as institutions, do not provide protection to investors' investment from these entities' failures and do not have access to central banks' liquidity facilities. To the extent that shadow banking entities carry out banking activities, exposures to such entities may therefore be inherently risky - and thus specific limits for individual and aggregate exposures are warranted.

28. Macro prudentially, institutions' exposures to shadow banking entities could be of concern for different reasons. Here the focus is on the role that institutions' funding of bank-like activity amongst shadow banking entities may play in increasing systemic risk across the financial system. One concern is that institutions' funding of large amounts of bank-like activity amongst shadow banking entities may result in an amplification of the credit cycle. Such a concern may arise from the observation that the flow of funds into such entities tends to be volatile. Moreover, the sharp accelerations of credit flows (and implicit exposures) into these entities can result in volatile (and potentially unsustainable) credit flows into the real economy. A limit on institutions' aggregate exposures to shadow banking entities could play a role in reducing the volatility of such flows.

29. Notwithstanding these microprudential and macroprudential risks, the EBA recognises that banking activities by some shadow banking entities can play a valuable role in providing alternative sources of funding to the real economy. Excessively reducing the availability of institutions' funding to these entities could therefore interfere with the flow of funds into the real economy. Moreover, the regulatory bodies, in the EU and at the global level, are still in the process of assessing the balance of risks and benefits that institutions' funding to different types of shadow banking entities represents. It is therefore considered premature to use the guidelines to introduce a quantitative limit to institutions' exposures to these entities at the individual or aggregate exposure level. Instead, the proposed intervention is designed to place the responsibility on the banking sector to demonstrate that the risks highlighted above are being managed effectively, in particular by improving, where necessary, the due diligence carried out before taking lending decisions, for instance to identify if the counterparty is carrying out credit intermediation and its regulatory status (see also sub-section 2.1.1, *Concerns regarding shadow banking entities*).

30. Under the guidelines, institutions should implement effective processes, as well as set internal aggregate and individual limits to exposures to individual shadow banking entities with an exposure value, after credit risk mitigation and exemptions, equal to or in excess of 0.25% of the institution's eligible capital as defined in Article 4(1)(71) of Regulation (EU) No 575/2013. The

materiality threshold of 0.25% of the institution's eligible capital reduces the burden of application of the guidelines, as it allows institutions to disregard immaterial exposures which are not likely to pose risks that would deserve special attention. The data collection accompanying these guidelines has shown that the number of exposures below this materiality threshold is very significant for most institutions: these exposures represent around 97% of the total number of exposures for the overall sample of institutions in the data collection.

31. The internal limits should be set using criteria which are laid down in the guidelines. The rationale for this approach ('the principal approach') is to make sure institutions have sufficient information about their counterparties in the shadow banking sector to make an informed assessment of their risk exposures to shadow banking entities as a whole, as well as of any individual exposure to shadow banking entities. It shall be noted that there is no necessary sequence for the setting of limits: i.e. institutions have to set both aggregate and individual limits, in any order.
32. Institutions that cannot use the principal approach for setting the internal limits as a result of their inability to take into account all the criteria, due to either an insufficient level of information about their exposures to shadow banking entities or the lack of effective processes to use that information, shall use an alternative approach ('the fallback approach') involving a set aggregate limit to all or some of their exposures to shadow banking entities. Where institutions can meet the requirements regarding effective processes and control mechanisms or oversight by their management board as set out in Section 4 of the guidelines, but cannot gather sufficient information to enable them to set out appropriate limits as set out in Section 5 of the guidelines, the fallback approach should only be applied to the exposures to shadow banking entities for which the institutions are not able to gather sufficient information. The principal approach should be applied to the remaining exposures to shadow banking entities.
33. Although the results of the data collection provided relevant input to the calibration of the aggregate limit under the fallback approach, the EBA notes some important differences between the data collection and the guidelines: the scope of the data collection was broader than the current scope of the guidelines²⁴; the data collection was conducted at the highest level of consolidation in a Member State or individual level if the consolidated level did not apply; and

²⁴ The data collection used the same definition of 'shadow banking entities' as included in the guidelines, with the following exceptions, where more granular data was collected:

- a. The list of 'excluded undertakings' considered for the definition of 'shadow banking entity' in the guidelines extends beyond the one considered for the data collection (i.e. points (k), (m), (n), (o), and (p) of the list in the guidelines have not been considered 'excluded undertakings' for the purposes of the data collection). For example, institutions have been asked to report exposures to all investment funds, regardless of whether they are subject to the UCITS Directive or the AIFMD. Note that UCITS funds (other than money market funds) and alternative investment funds that meet certain requirements have been excluded from the scope of the guidelines.
- b. Institutions have been asked to report exposures to all third party undertakings. Note that undertakings which are not supervised on a solo level, but supervised on a consolidated level in the Union or in a third country which has a regime at least equivalent to the one applied in the Union, have been excluded from the scope of the guidelines.

data simulations were done under the conservative assumption that the institution would apply the fallback approach to all of its exposures.

34. The main purpose of the fallback approach is to create certainty about the possibility of setting a limit for any institution; in particular, some institutions may not be able to apply all of the relevant criteria to use the principal approach. In that sense, the limit in the fallback approach can be seen as a way to ensure that these institutions apply a sufficiently tight limit to their exposures to shadow banking entities, for which institutions are not able to collect sufficient information that would enable them to understand and manage the risks of these exposures. The fallback approach can also work as an incentive for these institutions to improve their processes and control mechanisms concerning their exposures to shadow banking entities in order to be able to apply the criteria under the 'principal approach' to all their exposures to shadow banking entities.
35. All in all, the approach proposed in these guidelines requires institutions to set risk tolerance levels for exposures to shadow banking entities within their overall business model and risk management framework, under the supervision of the competent authority. In this regard, it is recognised that some institutions may have a higher risk appetite for these types of exposures and this can be accommodated within the guidelines once risks arising from these exposures are identified and appropriately mitigated. Given this, these guidelines are a first step to address the potential risks stemming from exposures to shadow banking entities. As already mentioned, the EBA has collected data about exposures to shadow banking entities in order to inform further work to be done on the topic by the Commission in accordance with its mandate under the last subparagraph of Article 395(2) of Regulation (EU) No 575/2013. The results of this data collection are presented in a separate report. As part of this mandate, the Commission may choose to propose imposing mandatory limits to exposures to shadow banking entities that are tighter than the limits currently laid down for large exposures in general. In any case, the EBA expects these guidelines to be a useful input to the Commission's report.
36. Under this approach, competent authorities will retain the ability to take supervisory measures to address any risks arising from exposures to shadow banking entities, as appropriate, and in particular to assess and challenge the internal limits and risk mitigation plans set by institutions.
37. The competent authorities' assessment will be guided by the SREP under Article 97 of Directive 2013/36/EU and in particular the technical criteria for the supervisory review and evaluation of exposure to and management of concentration risk by institutions under Article 98 of the same directive. Where it is deemed appropriate, consideration shall be given to the assignment of potential Pillar 2 requirements on specific institutions and, where necessary, competent authorities may also impose additional requirements under Article 104 of Directive 2013/36/EU where the risks arising from excessive exposures to shadow banking entities are not appropriately mitigated. The guidelines aim to provide a more structured basis for supervisors to make such Pillar 2 judgements within the supervisory review process in relation to exposures to shadow banking entities.

38. The combination of the chosen approach within the guidelines with the parallel option for supervisors to apply existing Pillar 2 measures in certain cases will allow the right balance to be found between allowing institutions to set their risk appetite for exposures to shadow banking entities and ensuring that their exposure does not result in excessive risk to the financial system.



3. Guidelines

EBA/GL/20XX/XX

DD Month YYYY

Guidelines

Limits on exposures to shadow banking entities which carry out banking activities outside a regulated framework under Article 395(2) of Regulation (EU) No 575/2013

1. Compliance and reporting obligations

Status of these guidelines

1. This document contains guidelines issued pursuant to Article 16 of Regulation (EU) No 1093/2010²⁵. In accordance with Article 16(3) of Regulation (EU) No 1093/2010, competent authorities and financial institutions must make every effort to comply with the guidelines.
2. Guidelines set out the EBA's view of appropriate supervisory practices within the European System of Financial Supervision or of how Union law should be applied in a particular area. Competent authorities as defined in Article 4(2) of Regulation (EU) No 1093/2010 to whom guidelines apply should comply by incorporating them into their practices as appropriate (e.g. by amending their legal framework or their supervisory processes), including where guidelines are directed primarily at institutions.

Reporting requirements

3. According to Article 16(3) of Regulation (EU) No 1093/2010, competent authorities must notify the EBA as to whether they comply or intend to comply with these guidelines, or otherwise with reasons for non-compliance, by ([dd.mm.yyyy]). In the absence of any notification by this deadline, competent authorities will be considered by the EBA to be non-compliant. Notifications should be sent by submitting the form available on the EBA website to compliance@eba.europa.eu with the reference 'EBA/GL/201x/xx'. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authorities. Any change in the status of compliance must also be reported to the EBA.
4. Notifications will be published on the EBA website, in line with Article 16(3) of Regulation (EU) No 1093/2010.

²⁵ Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12).

2. Subject matter, scope and definitions

Subject matter

5. These guidelines specify the methodology that should be used by institutions, as part of their internal processes and policies, for addressing and managing concentration risk arising from exposures to shadow banking entities. In particular, these guidelines specify criteria for setting an appropriate aggregate limit on exposures to shadow banking entities which carry out banking activities outside a regulated framework, as well as individual limits on exposures to such entities.

Scope of application

6. These guidelines fulfil the mandate given to the EBA under Article 395(2) of Regulation (EU) No 575/2013²⁶.
7. These guidelines build in particular on Articles 73 and 74 of Directive 2013/36/EU²⁷, which require institutions to have sound, effective and comprehensive strategies and processes to assess and maintain on an ongoing basis the amounts, types and distribution of internal capital that they consider adequate to cover the nature and level of the risks to which they are or might be exposed, as well as effective processes to identify, manage, monitor and report such risks and adequate internal control mechanisms; and Articles 97 and 103 of Directive 2013/36/EU, which establish that competent authorities must review the arrangements, strategies, processes and mechanisms implemented by institutions to comply with Regulation (EU) No 575/2013 and Directive 2013/36/EU, and evaluate the risks to which the institutions are or might be exposed, and that they may apply the supervisory review and evaluation process (SREP) to institutions which are or might be exposed to similar risks or pose similar risks to the financial system.
8. These guidelines apply to exposures to shadow banking entities as defined below.
9. These guidelines apply to institutions to which Part Four of Regulation (EU) No 575/2013 (Large Exposures) applies, in accordance with the level of application set out in Part I, Title II, of that Regulation.

²⁶ Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) no 648/2012 (OJ L 321, 30.11.2013, p. 6).

²⁷ Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

Addressees

10. These guidelines are addressed to competent authorities as defined in point (i) of Article 4(2) of Regulation (EU) No 1093/2010 and to financial institutions as defined in Article 4(1) of Regulation No 1093/2010.

Definitions

11. Unless otherwise specified, terms used and defined in Regulation (EU) No 575/2013 and Directive 2013/36/EU have the same meaning in the guidelines. In addition, for the purposes of these guidelines, the following definitions apply:

<p><i>Credit intermediation activities</i></p>	<p>Bank-like activities involving maturity transformation, liquidity transformation, leverage, credit risk transfer or similar activities.</p> <p>These activities include at least those listed in the following points of Annex 1 of Directive 2013/36/EU: points 1 to 3, 6 to 8, and 10.</p>
<p><i>Exposures to shadow banking entities</i></p>	<p>Exposures to individual shadow banking entities pursuant to Part Four of Regulation (EU) No 575/2013 with an exposure value, after taking into account the effect of the credit risk mitigation in accordance with Articles 399 to 403 and exemptions in accordance with Articles 400 and 493(3) of that Regulation, equal to or in excess of 0.25% of the institution's eligible capital as defined in Article 4(1)(71) of Regulation (EU) No 575/2013.</p>
<p><i>Shadow banking entities</i></p>	<p>Undertakings that carry out one or more credit intermediation activities and that are not excluded undertakings.</p>
<p><i>Excluded undertakings</i></p>	<p>(1) undertakings included in consolidated supervision on the basis of the consolidated situation of an institution as defined in Article 4(1)(47) of Regulation (EU) No 575/2013.</p> <p>(2) undertakings which are supervised on a consolidated basis by a third country competent authority pursuant to the law of a third country</p>



which applies prudential and supervisory requirements that are at least equivalent to those applied in the Union.

(3) undertakings which are not within the scope of points (1) and (2) but which are:

(a) credit institutions;(b) investment firms;

(c) third country credit institutions if the third country applies prudential and supervisory requirements to that institution that are at least equivalent to those applied in the Union;

(d) recognised third country investment firms;

(e) entities which are financial institutions authorised and supervised by the competent authorities or third country competent authorities and subject to prudential requirements comparable to those applied to institutions in terms of robustness where the institution's exposure(s) to the entity concerned is treated as an exposure to an institution pursuant to Article 119(5) of Regulation (EU) No 575/2013;

(f) entities referred to in points (2) to (23) of Article 2(5) of Directive 2013/36/EU;

(g) entities referred to in Article 9(2) of Directive 2013/36/EU;

(h) insurance holding companies, insurance undertakings, reinsurance undertakings and third country insurance undertakings and third-country reinsurance undertakings where the supervisory regime of the third country concerned is deemed equivalent;

(i) undertakings excluded from the scope of Directive 2009/138/EC²⁸ in accordance with

²⁸ Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of insurance and reinsurance (Solvency II) (recast) (OJ L 335, 17.12.2009, p. 1).



Article 4 of that Directive;

(j) institutions for occupational retirement provision within the meaning of point (a) of Article 6 of Directive 2003/41/EC²⁹ or subject to prudential and supervisory requirements comparable to those applied to institutions within the meaning of point (a) of Article 6 of Directive 2003/41/EC in terms of robustness;

(k) undertakings for collective investment:

(i) within the meaning of Article 1 of Directive 2009/65/EC³⁰;

(ii) established in third countries where they are authorised under laws which provide that they are subject to supervision considered to be equivalent to that laid down in Directive 2009/65/EC;

(iii) within the meaning of Article 4(1)(a) of Directive 2011/61/EU³¹ with the exception of:

- undertakings employing leverage on a substantial basis according to Article 111(1) of Commission Delegated Regulation (EU) 231/2013³² and/or
- undertakings which are allowed

²⁹ Directive 2003/41/EC of the European Parliament and of the Council of 3 June 2003 on the activities and supervision of institutions for occupational retirement provision (OJ L 235, 23.9.2003, p. 10).

³⁰ Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS) (recast) (OJ L 302, 17.11.2009, p. 32).

³¹ Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010 (OJ L 174, 1.7.2011, p. 1).

³² Commission Delegated Regulation (EU) No 231/2013 of 19 December 2012 supplementing Directive 2011/61/EU of the European Parliament and of the Council with regard to exemptions, general operating conditions, depositaries, leverage, transparency and supervision (OJ L 83, 22.3.2013, p. 1).



to originate loans or purchase third party lending exposures onto their balance-sheet pursuant to the relevant fund rules or instruments of incorporation;

(iv) which are authorised as ‘European long-term investment funds’ in accordance with Regulation (EU) 2015/760³³;

(v) within the meaning of Article 3 (1)(b) of Regulation (EU) 346/2013³⁴ (‘qualifying social entrepreneurship funds’);

(vi) within the meaning of Article 3(b) of Regulation (EU) 345/2013³⁵ (‘qualifying venture capital funds’).

except undertakings that invest in financial assets with a residual maturity not exceeding two years (short-term assets) and have as distinct or cumulative objectives offering returns in line with money market rates or preserving the value of the investment (money market funds);

(l) central counterparties (CCPs) as defined in point (1) of Article 2 of Regulation (EU) No 648/2012³⁶ established in the EU and third country CCPs recognised by ESMA pursuant to

³³ Regulation (EU) 2015/760 of the European Parliament and of the Council of 29 April 2015 on European long-term investment funds (OJ L 123, 19.5.2015, p. 98).

³⁴ Regulation (EU) No 346/2013 of the European Parliament and of the Council of 17 April 2013 on European social entrepreneurship funds (OJ L 115, 25.4.2013, p. 18).

³⁵ Regulation (EU) No 345/2013 of the European Parliament and of the Council of 17 April 2013 on European venture capital funds (OJ L 115, 25.4.2013, p. 1).

³⁶ Regulation (EU) 648/2012 of European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).



Article 25 of that Regulation;

(m) electronic money issuers as defined in point (3) of Article 2 of Directive 2009/110/EC³⁷;

(n) payment institutions as defined in point (4) of Article 4 of Directive 2007/64/EC³⁸;

(o) entities the principal activity of which is to carry out credit intermediation activities for their parent undertakings, for their subsidiaries or for other subsidiaries of their parent undertakings;

(p) resolution authorities, asset management vehicles and bridge institutions as defined in points (18), (56) and (59) of Article 2(1) of Directive 2014/59/EU³⁹ and entities wholly or partially owned by one or more public authorities established prior to the 1 January 2016 for the purpose of receiving and holding some or all of the assets, rights and liabilities of one or more institutions in order to preserve or restore the viability, liquidity or solvency of an institution or to stabilise the financial market.

³⁷ Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (OJ L 267, 10.10.2009, p. 7).

³⁸ Directive 2007/64/EC of the European Parliament and of the Council of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (OJ L 319, 5.12.2007, p. 1).

³⁹ Directive 2014/59/EU of the European Parliament and of the Council of 15 May 2014 establishing a framework for the recovery and resolution of credit institutions and investment firms and amending Council Directive 82/891/EEC, and Directives 2001/24/EC, 2002/47/EC, 2004/25/EC, 2005/56/EC, 2007/36/EC, 2011/35/EU, 2012/30/EU and 2013/36/EU and Regulations (EU) No 1093/2010 and (EU) No 648/2012 of the European Parliament and of the Council (OJ L 173, 12.6.2014, p.190).

3. Implementation

Date of application

12. These guidelines apply from 01.01.2017.

4. Requirements regarding limits to exposures to shadow banking entities

13. Institutions should comply with the general principles referred to in this section, as well as set limits as referred to under Section 5, as applicable.

Effective processes and control mechanisms

14. Institutions should:

- a. Identify their individual exposures to shadow banking entities, all potential risks to the institution arising from those exposures, and the potential impact of those risks.
- b. Set out an internal framework for the identification, management, control and mitigation of the risks outlined in point a). This framework should include clearly defined analyses to be performed by risk officers regarding the business of a shadow banking entity to which an exposure arises, the potential risks to the institution and the likelihood of contagion stemming from these risks to the entity. Those analyses should be performed under the supervision of the credit risk committee, which should be duly informed of the results.
- c. Ensure that risks outlined in letter a) are adequately taken into account within the institution's Internal Capital Adequacy Assessment (ICAAP) and capital planning.
- d. Based on the assessment conducted under letter a), set the institution's risk tolerance/risk appetite for exposures to shadow banking entities.
- e. Implement a robust process for determining interconnectedness between shadow banking entities, and between shadow banking entities and the institution. This process should in particular address situations where interconnectedness cannot be determined, and set out appropriate mitigation techniques to address potential risks stemming from this uncertainty.
- f. Have effective procedures and reporting processes to the management body regarding exposures to shadow banking entities within the institution's overall risk management framework.
- g. Implement appropriate action plans in the event of a breach of the limits set by the institution in accordance with Section 5.

Oversight by the management body of the institutions

15. When overseeing the application of the principles referred to above as well as the application of limits set out in accordance with the principal approach in Section 5, the institution's management body should, on a regular predetermined basis:
 - a. review and approve the institution's risk appetite to exposures to shadow banking entities and the aggregate and individual limits set in line with Section 5;
 - b. review and approve the risk management process to manage exposures to shadow banking entities, including analysis of risks arising from those exposures, risk mitigation techniques and potential impact on the institution under stressed scenarios;
 - c. review the institution's exposures to shadow banking entities (on an aggregate and individual basis) as a percentage of total exposures and expected and incurred losses;
 - d. ensure the setting of the limits referred to in these guidelines is documented, including any changes to them.

16. The institution's management body may delegate the reviews set out in paragraph 15 a) to d) to senior management.

5. Principal approach for setting limits to exposures to shadow banking entities

Setting an aggregate limit on exposures to shadow banking entities

17. Institutions should set an aggregate limit to their exposures to shadow banking entities relative to their eligible capital.
18. When setting an aggregate limit to exposures to shadow banking entities, each institution should take into account:
 - a. its business model, risk management framework as outlined in paragraph 14b), and risk appetite as outlined in paragraph 14d);
 - b. the size of its current exposures to shadow banking entities relative to its total exposures and relative to its total exposure to regulated financial sector entities;
 - c. interconnectedness as outlined in paragraph 14e).

Setting individual limits on exposures to shadow banking entities

19. Independently of the aggregate limit, and in addition to it, institutions should set tighter limits on their individual exposures to shadow banking entities. When setting those limits, as part of their internal assessment process, the institutions should take into account:
 - a. the regulatory status of the shadow banking entity, in particular whether it is subject to any type of prudential or supervisory requirements;
 - b. the financial situation of the shadow banking entity including, but not limited to, its capital position, leverage and liquidity position;
 - c. information available about the portfolio of the shadow banking entity, in particular non-performing loans;
 - d. available evidence about the adequacy of the credit analysis performed by the shadow banking entity on its portfolio, if applicable;
 - e. whether the shadow banking entity will be vulnerable to asset price or credit quality volatility;
 - f. concentration of credit intermediation activities relative to other business activities of the shadow banking entity;
 - g. interconnectedness as outlined in paragraph 14 e);
 - h. any other relevant factors identified by the institution under paragraph 14 a).

6. Fallback approach

20. If institutions are not able to apply the principal approach as set out in Section 5, their aggregate exposures to shadow banking entities should be subject to the limits on large exposures in accordance with Article 395 of Regulation (EU) No 575/2013 (including the use of Article 395(5) of the same Regulation) ('the fallback approach').
21. The fallback approach should be applied in the following way:
- a) If institutions cannot meet the requirements regarding effective processes and control mechanisms or oversight by their management body as set out in Section 4, they should apply the fallback approach to all their exposures to shadow banking entities (i.e. the sum of all their exposures to shadow banking entities).
 - b) If institutions can meet the requirements regarding effective processes and control mechanisms or oversight by their management body as set out in Section 4, but cannot gather sufficient information to enable them to set out appropriate limits as set out in Section 5, they should only apply the fallback approach to the exposures to shadow banking entities for which the institutions are not able to gather sufficient information. The principal approach as set out in Section 5 should be applied to the remaining exposures to shadow banking entities.

4. Accompanying documents

4.1 Cost-Benefit Analysis/Impact Assessment⁴⁰

4.1.1 Problem identification

The interconnectedness between the (regulated) banking sector and shadow banking entities and the specific risks posed by shadow banking entities to the stability of the financial system provide the motivation for action to be taken with regard to institutions' exposures to shadow banking entities.

Under the current regulatory regime, institutions' exposures to shadow banking entities are already subject to limits under the general framework for large exposures. However, the general framework for large exposures could be supplemented by provisions that would be specific to the monitoring and limiting of exposures to shadow banking entities, given the risks they might entail. To set such a framework, a set of decisions must be made regarding the scope of the application of the guidelines (in particular the definition of shadow banking entities) and the limits to be set.

4.1.2 Policy objectives

The present guidelines are intended to fulfil the regulatory objectives of (a) mitigating microprudential risk (i.e. risks posed to institutions as a result of their exposures to shadow banking entities), (b) mitigating macroprudential risks (e.g. financial stability) and (c) mitigating regulatory arbitrage risks (i.e. between the regulated and unregulated parts of the financial system). To achieve the regulatory objectives, the guidelines target specific and operational objectives. In particular, the guidelines aim to specify the scope of their application (specific objective), the definition of shadow banking entities (operational objective to meet the specific objective of the scope of application) and the types of limits which might be set (specific objective).

The legal mandate in Article 395(2) of Regulation (EU) No 575/2013 requires the EBA to issue guidelines to set appropriate aggregate limits to shadow banking exposures or tighter individual limits on exposures to shadow banking entities which carry out banking activities outside a regulated framework, taking into account any material detrimental impact on the provision of credit to the real economy or on the stability of financial markets.

⁴⁰ The analysis in this section is partly based on information collected in a dedicated exercise and presented in more detail in the EBA Report on institutions' exposures to shadow banking entities (2015).



4.1.3 Options considered

First set of options (specific): scope of application/definition of shadow banking entities

The legal mandate requires the EBA to set limits on exposures to shadow banking entities which carry out banking activities outside a regulated framework.

As a starting point, the EBA considers that ‘banking activities’ should be interpreted as activities involving maturity transformation, liquidity transformation, leverage, credit risk transfer or similar credit intermediation activities. To provide guidance to institutions the EBA suggests that these activities include at least those listed in points 1 to 3, 6 to 8 and 10 of Annex 1 of Directive 2013/36/EU. This is consistent with the approach adopted in international (in particular FSB) and other European contexts.

As for the interpretation of ‘regulated framework’, two key elements were considered: (i) the inclusion in prudential consolidation and supervision and (ii) specific solo prudential and conduct regulatory frameworks.

First, as regards the treatment of *entities within the scope of prudential consolidation* the following options were considered:

- a. **Option 1.1:** Entities which are subject to prudential supervision on the basis of the consolidated situation of an institution as defined in Article 4(1)(47) of Regulation (EU) No 575/2013 should be outside the definition of shadow banking entities only if they are also subject to solo prudential requirements which are at least equivalent to Regulation (EU) No 575/2013 and Directive 2013/36/EU.
- b. **Option 1.2:** Entities which are subject to prudential supervision on the basis of the consolidated situation of an institution as defined in Article 4(1)(47) of Regulation (EU) No 575/2013 should be outside the definition of shadow banking entities regardless of whether they are subject to solo prudential requirements which are at least equivalent to Regulation (EU) No 575/2013 and Directive 2013/36/EU.

Preferred option: Option 1.2 is preferable, as any such entities carrying out credit intermediation activities would be subject to prudential requirements at the consolidated level as a result of prudential consolidation, thereby mitigating any risks posed by the bank-like activities carried out by those entities. Given this, these entities should not be regarded as being ‘outside a regulated framework’ and therefore should be carved out from the definition of shadow banking entities.

Second, for those *entities that are not subject to prudential consolidation*, the EBA considered different types of regulatory frameworks. In particular, two options were considered:

- a. **Option 2.1:** Institutions subject to third country prudential and supervisory requirements or other Union or national prudential frameworks, which are at least equivalent to Regulation (EU) No 575/2013 and Directive 2013/36/EU should be carved out from the definition of shadow banking entities.



- b. **Option 2.2:** Entities subject to any regulatory framework (of a prudential or conduct nature) under Union law or equivalent third country or national law for institutions and other regulated entities should be carved out from the definition of shadow banking entities.

Preferred option: Having regard to the objectives identified in the section above, the focus of the policy debate on shadow banking in Union and international contexts, the need for EBA to act in a manner that is consistent and coherent with Union initiatives in the field of financial regulation, and the need for EBA to adopt a risk-based proportionate approach to regulation, the EBA considers that Option 2.1 is the only reasonable approach to interpretation for the purposes of the guidelines. Under that approach, such a 'regulated framework' is understood as a robust prudential regulation framework where credit, liquidity, leverage and other risks are adequately addressed.

The approach under Option 2.2, on the other hand, would exclude entities that are, for example, subject to a light touch or non-prudential regime which may fail to mitigate effectively risks posed by the carrying out of credit intermediation by the entity concerned.

The proposed approach, in contrast, would focus on entities that are not subject to an appropriate prudential framework, thereby concentrating on those entities that pose the greatest risks in terms of both the direct exposures institutions face and, more widely, the incentives for credit intermediation to be carried out outside the regulated framework.

According to the results of the dedicated data collection, only slightly more than 10% of the exposure amounts are to entities which are known to be supervised on a consolidated level in the Union or in a third country with an at least equivalent prudential regime. For almost 90% of the exposure amounts, the type of supervision of the counterparty is not known or not further specified. From a prudential perspective, this result justifies the option chosen above, as only a minor proportion of the exposure amounts is known to be supervised on a consolidated level and can consequently be reasonably carved out from the scope of application of these guidelines.

Turning specifically to the treatment of funds, these tend to engage in maturity and liquidity transformation and are generally regarded as outside the traditional banking sector. Therefore, *prima facie*, they should be within the scope of the definition of shadow banking entity. However, some funds are regulated pursuant to prudential frameworks similar to those applied to credit institutions and investment firms and should therefore be excluded from the scope of the guidelines. Based on the results of the data collection, the proportion of amounts of exposures (after taking into account credit risk mitigation and exemptions) to MMFs (UCITS and others) is rather small (< 5% of total exposure amounts). Around one quarter of the exposure amounts is to (non-MMF) investment funds, out of which one fifth is to hedge funds.



Second set of options (specific): establishment of limits

After assessing the objectives of the limits to be developed and the concerns to be addressed, EBA has identified three possible policy options (see 3.1 to 3.3 below).

- a) **Option 3.1:** Explicit appropriate aggregate limits or tighter individual limits on exposures to shadow banking entities under Pillar 1

Setting tighter individual limits (i.e. an exposure limit lower than the large exposure limit of 25% of an institution's eligible capital after taking into account the effect of credit risk mitigation measures) or appropriate aggregated limits on exposures to individual shadow banking entities would be a very direct way to limit the regulated banking sector's exposures to shadow banking entities. When setting individual limits, different types of shadow banking entities, activities or instruments could be considered.

Given that any regulatory proposal about quantitative limits on exposures to shadow banking entities needs to be based on a thorough impact analysis, the EBA finds it premature to set out limits to individual or aggregate exposures to shadow banking entities. Simultaneously with issuing these guidelines, EBA is publishing an in-depth report to inform the Commission on European credit institutions' and investment firms' exposures to shadow banking entities. Based on that analysis, the co-legislators may decide on any harder limits in accordance with Article 395(2) of the CRR, after having assessed the appropriateness and impact of regulatory measures.

- b) **Option 3.2:** Individual limits on exposures to shadow banking entities to be set by institutions

To the extent that shadow banking entities carry out banking activities, such as maturity and liquidity transformation, which are inherently risky, exposures to such entities may therefore also be inherently risky - and thus specific limits for individual and aggregate exposures are warranted (see further reasoning in section 2.1.4, *Rationale for limiting institutions' exposures to shadow banking entities*).

This approach could be understood as forming part of the Pillar 2 framework. It should be noted that concentration risk is clearly identified as a core part of the Supervisory Review Process within the Capital Requirement Directive.⁴¹ Where a concentration risk to shadow banking entities was identified, then a capital add-on, or additional obligation on a bank's funding/liquidity structure, may be warranted.⁴²

⁴¹ See Directive 2013/36/EU – Section III, Article 98(1)(b).

⁴² It should be noted that, in the Basel Capital Framework (and the CRD), concentration risk is not fully addressed in the context of Pillar 1. For credit risk it is assumed that IRB portfolios are perfectly diversified. Any resultant underestimation of risk should be corrected by addressing the concentration risk and allocating capital, where necessary. For details see the EBA guidelines on concentration risk: <https://www.eba.europa.eu/documents/10180/16094/Concentration.pdf>.



- c) **Option 3.3:** Aggregate limits on exposures to shadow banking entities to be set by the institutions

The interconnectedness between the shadow banking and the regulated banking sector, plus the tendency of shadow banking entities to engage in excessively leveraged or otherwise risky activities, calls for management of exposures not only to individual shadow banking entities, but also to the shadow banking sector in its entirety.

Institutions may have an incentive to shift activities to the shadow banking sector in response to more stringent capital requirement. Also, periods of low real interest rates may fuel such a tendency as demand from institutional cash pools for alternative investment opportunities grows and the 'search for yield' phenomenon accelerates funds into the shadow banking sector. An overall backstop limit, together with improved identification of large exposures connected to the shadow banking sector, would help safeguard the regulated banking sector, preventing it from overly fuelling the growth of the unregulated shadow banking sector (thus getting overly interlinked and exposed).

The EBA sees that an aggregate limit to the shadow banking sector will result in a net benefit to the economy. From a macroprudential perspective, this approach should ensure that the shadow banking sector remains able to provide credit to the real economy without creating excessive risks to financial stability (including spillover risk). The institutions would set their aggregate limit to the aggregate of shadow banking entities, in the same way as described in Option 3.2.

If the approach under Options 3.2 and 3.3 ('the principal approach') cannot be applied, a 'fallback approach' would be applied, whereby a specific limit would be applied for the aggregate exposures to shadow banking entities. The report on institutions' exposures to shadow banking entities shows the distribution of institutions into different clusters by their exposure to the shadow banking sector. The following technical specifications are considered fallback solutions:

Option 3.3.a: If institutions cannot meet the requirements regarding effective processes and control mechanisms or oversight by their management board, regardless of whether they can gather sufficient information about their individual exposures they should apply the fallback approach to all their exposures to shadow banking entities (i.e. the sum of all their exposures to shadow banking entities).

Option 3.3.b: If institutions can meet the requirements regarding effective processes and control mechanisms or oversight by their management board, but cannot gather sufficient information regarding one or more individual exposures, they should apply the fallback approach to all their exposures to shadow banking entities (i.e. the sum of all their exposures to shadow banking entities), regardless of whether the institutions are able to gather sufficient information on some exposures.

Option 3.3.c: If institutions can meet the requirements regarding effective processes and control mechanisms or oversight by their management board, but cannot gather sufficient information regarding one or more individual exposures, they should only apply the fallback approach to the



exposures to shadow banking entities for which the institutions are not able to gather sufficient information. The principal approach should be applied to the remaining exposures to shadow banking entities.

Preferred options: After deliberating all pros and cons from a prudential perspective and having regard to the feedback received during the public consultation, the EBA proposes to combine Options 3.2 and 3.3. Institutions should both set an aggregate limit to their exposure to the shadow banking entities and also set tighter limits to individual exposures to shadow banking entities. In addition, institutions unable to implement effective processes and control mechanisms or to ensure oversight by their management board should apply the fallback approach to all their exposures (Option 3.3a). However, if institutions can meet these requirements and can gather relevant information about one or more individual counterparties from the shadow banking sector, this would be recognised and the fallback approach would apply only to the exposures for which the institution has not been able to collect sufficient information (Option 3.3c).

In addition, for the purposes of the application of the guideline, institutions could either:

- a) **Option 4.1:** consider only exposures, after taking into account credit risk mitigation techniques and exemptions, with a value equal to or in excess of 0.25% of the institution's eligible capital; or
- b) **Option 4.2:** consider all exposures to shadow banking entities.

Option 4.1 is consistent with other EBA products in the area of large exposures⁴³ and would significantly alleviate the burden for institutions and is therefore proposed as the preferred option. Although some caution needs to be exerted when interpreting the reported data, the EBA's dedicated analysis estimates that around 97% of the number of exposures reported by institutions in the sample are below this materiality threshold, which alleviates considerably the burden of compliance with the guidelines.

4.1.4 Cost-benefit analysis

The EBA conducted a comprehensive data collection to better understand the relevance and characteristics of institutions' exposures to shadow banking entities and also to support the development and policy choices of these guidelines. Based on that data collection, the costs for credit institutions, the credit provided to financial counterparties and the real economy and the benefits for the solvency of individual institutions and the stability of the financial system are estimated in a separate report. For the purpose of the Commission's assessment of the appropriateness of imposing regulatory limits, that report also contains a comprehensive analysis of institutions' exposures to shadow banking entities.

⁴³ EBA Final Draft Regulatory Technical Standards on the determination of the overall exposure to a client or a group of connected clients in respect of transactions with underlying assets under Art. 390(8) of Regulation (EU) No 575/2013.



Concerning the impact on the risk profile of credit institutions and investment firms, the results of the dedicated data analysis confirm that the number of exposures above common large exposure thresholds (e.g. 10% for reporting requirements, 25% for quantitative restrictions) is rather small. Relative to their eligible capital, average individual exposures are significantly higher (a multiple) for small and/or domestic institutions (Group 2 banks) and investment firms than for large and internationally active banks (Group 1). These guidelines should contribute to improved risk management and more comprehensive counterparty information collection. Requirements for individual and aggregate limits can be reasonably expected to contribute to less concentration risk towards shadow banking entities/the shadow banking sector for both Group 1 and Group 2 banks as well as investment firms. The majority of institutions' qualitative responses to the data collection associate exposures to shadow banking entities with above-average risk weights. Around a quarter of institutions associate higher revenues with shadow banking exposures and estimate the overall impact of their replacement by other exposures to be rather costly in profitability terms.

The potential detrimental impact on the provision of credit to the real economy in the EU is expected to be small (to medium) and carefully managed by the design of these guidelines. The results of the dedicated data collection show that around half of the amount of funds provided by European institutions is to counterparties resident outside the EU. It is rather unlikely that those funds would be finally destined for financing the real economy in the EU. Further, a certain proportion of those funds is provided to types of counterparty which are far less likely to focus on the direct provision of credit to the real economy. Thus the potential detrimental impact of limiting exposures to hedge funds, MMFs or broker-dealers is expected to be rather small. Lastly, the restriction of the application of these guidelines to exposure values after taking into account credit risk mitigation and exemptions, exposures to counterparties not (known to be) equivalently supervised at consolidated level, the qualitative principle-oriented approach of these guidelines and the application of a materiality threshold have all been designed to mitigate any potential detriment to the provision of credit to the real economy.

The direct and indirect beneficial impact on the stability and orderly functioning of financial markets in the EU is expected to be medium to high. Firstly, the largest part of European institutions' exposures to shadow banking entities is in the portfolio of Group 1 banks. Those, on average, exhibit higher exposures to the shadow banking sector in its entirety. Limiting concentrated exposures of institutions which are closer to being systemically important (because of their size and interconnectedness) to a potentially risky sector has benefits for financial stability. Similarly, certain types of counterparty entities are commonly perceived as carrying out risky activities (e.g. reliance on leverage, use of complex financial instruments) and being subject to relatively light prudential regulation (e.g. hedge funds). Limiting institutions' exposures to those counterparties which are also commonly perceived to behave in a correlated manner (e.g. invested in similar markets) can contribute to dampening procyclicality and systemic risk. Finally, the indirect approach of shadow banking regulation via tighter regulation of institutions' interaction with shadow banking entities can constitute a backstop to regulatory arbitrage. In summary, these guidelines are assumed to efficiently contribute to achieving the objectives stated above, while allowing for further regulatory intervention if considered appropriate.



4.2 Views of the Banking Stakeholder Group (BSG)

General comments

The consultation paper is an addition to other existing measures (such as SFT rules, haircut and reporting rules, etc.) that are designed to reduce systemic risk migration from the (largely unregulated) shadow banking sector to the highly regulated banking sector.

It is widely accepted that shadow banks of various sorts played an important role in the recent global banking crisis and that there were flaws in the way that such institutions operated and the links between the banking and shadow banking sectors. However, many of these flaws have since vanished as markets and institutions have reacted.

As a point of perspective, we also note that regulated banks are already subject to 'large exposure' rules irrespective of whether this relates to positions vis-à-vis banks or shadow banks. Furthermore, general capital requirements have been tightened up. Overall, these measures are likely to reduce the activity of banks vis-à-vis non-banks in general and shadow banks in particular.

The shadow banking landscape includes a heterogeneous set of institutions which cover a wide range of business activities and different business structures, and its size and functions can vary significantly between countries and markets. The shadow banking sector has a function in parallel with, and as a complement to, the banking system but on the other hand can create complexity and systemic risks. In addition, there is a risk of an undesirable risk transfer from the directly regulated sector to the shadow banking sector. The risk related to the shadow banking sector can to some extent be mitigated through indirect regulation, for example limitations for institutions to securitized assets, or as direct regulation towards shadow banking entities as example through AIFMD. Even if the indirect approach might have an impact in mitigating the risk in some areas, the view of BSG is that a more robust long term solution includes a regulation covering the shadow banking entities and its intermediation activities.

Before considering the specific questions raised in the consultation paper, we emphasise three general concerns. Firstly, there is a potential danger that the overall regulatory regime that is applied to regulated banks may not be as sufficiently competitively neutral as between institutions conducting essentially similar business and that this may unnecessarily distort competition between the regulated banking sector and the less-regulated institutions in the shadow banking sector.

A second concern is that regulatory agencies and national authorities should have a common definition of what is meant by 'shadow banks', and that regulation and supervision of the relationship between banks and shadow banks should be applied consistently between countries. This also raises issues of competitive neutrality between different national regulatory regimes.



Thirdly, the proposed rules outlined in the consultation paper may have the unintended consequence of undermining the fluidity of securitisation schemes that are currently proposed under the Capital Market Union: this may again produce regulatory inconsistencies.

Replies to questions

Q1. Do you agree with the approach the EBA has proposed for the purposes of defining shadow banking entities? In particular, do you consider that this approach is workable in practice? If not, please explain why and present possible alternatives.

In the FSB's 2014 Global Shadow Banking Monitoring Report, the shadow banking sector is defined as credit intermediation involving entities and activities outside the regular banking system or, as other market participants prefer, as 'market based activity'. This is a very broad definition and, in addition, the term carries a negative image. However, often this activity with non-bank financial institutions is carried out with institutions which are highly regulated, such as UCITS or insurance companies. As the consultation paper proposes increased control mechanisms towards shadow banking entities, a clear and operational definition is of great importance.

In this context we again emphasise the need for a common global definition of shadow banking.

The approach of defining entities that is out of scope for the definition of shadow banking is relevant and easy to adopt. In addition, the exposures towards UCITS are to a large extent already restricted by limits contained in the CRR. The most relevant approach for defining shadow banking entities seems to be by reference to the activities performed. Some of these are listed in the proposal with reference to CRD, annex 1. There is, nevertheless, considerable room for different translation of entities and activities in scope and the definitions still involve a high degree of subjectivity. Exposures to funds that are not considered as excluded undertakings should be possible to be treated by a look through principle where possible. It is also unclear how the exposure towards entities with mixed business lines should be treated in this context. As an example, should the total exposure towards an entity with some kind of shadow banking activity be considered as shadow banking in total when defining limits and interconnectedness?

The definition is broad and may generate a high number of 'positives', which could lead to an additional operational risk and disproportionate burden in terms of policies and control mechanisms, given that there would likely be only a relatively small overall risk reduction in the banking sector.

The view of the BSG is that the threshold of 0.25% is too low and the process of maintaining, monitoring and reporting these can be excessively administratively burdensome and disproportionate, considering turnover in portfolios and interconnectedness but also considering the fallback approach option 1 or option 2.

Q2. Do you agree with the approach the EBA has proposed for the purposes of establishing effective processes and control mechanisms? If not, please explain why and present possible alternatives.



The process will require specific instructions and monitoring and reporting requirements that are directly related to entities defined as shadow banking. Risk related to concentration and interconnectedness and specific risk towards specific entities is already an integrated part of the credit risk monitoring entity within most institutions and the need to set specific restrictions, at an institutional level towards a broad category of companies sorted into the category shadow banking, could be questioned. The definition of shadow banking entities includes intermediate activities, but in many cases this may be the only common denominator.

The proposed specific requirement for shadow banking entities related to Pillar 2 can be questioned, since the Pillar 2 requirements are already defined and in use already.

Q3. Do you agree with the approach the EBA has proposed for the purposes of establishing appropriate oversight arrangements? If not, please explain why and present possible alternatives.

It could be questioned if there is a need to have a specific process for exposures defined as being within the shadow banking definition. Risks, limits and risk appetite are an integral part of the credit risk monitoring and reporting process. However, we agree in principle with the arrangements.

Q4. Do you agree with the approaches the EBA has proposed for the purposes of establishing aggregate and individual limits? If not, please explain why and present possible alternatives.

An aggregated limit only has relevance if there is a defined interconnectedness between two or more entities in scope for the definition of shadow banking. There are potentially less combined risk and interconnectedness in exposures towards totally different shadow banking activities in different countries compared to some other interconnections which already should be considered following the large exposures regulation. Besides, indirect interconnectedness is difficult to assess in practice, for example if there are holdings by other institutions. With reference to no 18 of the consultation it is stated that the EBA is considering updating the 'Guidelines on the identification of groups of connected clients under Article 4, Para. 1, No 39 Regulation (EU) No 575/2013, including providing greater clarity on how institutions and special-purpose vehicles can be economically interdependent.'

The view of the BSG is that the review and updating of that guideline should be undertaken in parallel with the guideline on shadow banking. Furthermore, indirect interconnectedness is to some extent already addressed in the BCBS paper 'Supervisory framework for measuring and controlling large exposures', April 2014. Even though the Basel paper considers the identification of additional risk imposed by third parties by the structure the bank invests in (e.g. in the case of an originator, fund manager, liquidity provider or credit protection provider), there are remaining difficulties in identifying all those connections. Furthermore, the Basel paper remains vague in the case of structured finance products.

Q5. Do you agree with the fall back approach the EBA has proposed, including the cases in which it should apply? If not, please explain why and present possible alternatives. Do you think that Option 2 is preferable to Option 1 for the fall back approach? If so, why? In particular: Do you believe that Option 2 provides more incentives to gather information about exposures



than Option 1? Do you believe that Option 2 can be more conservative than Option 1? If so, when? Do you see some practical issues in implementing one option rather than the other?

The view of the BSG is that Option 2 is the preferred option, since the requirements for the main part of exposures are fulfilled and should not be affected by a small number of exposures where the criteria are not met. It would be to presume a very close linkage between normally rather heterogeneous entities that are treated as directly connected. The most conservative outcome of the different options should not be the main reason for preference and could basically be affected by just one minor exposure. However, a technical fallback is not necessarily the only approach to address shortcomings, as in the SPREP and by capital add-on.

4.3 Feedback on the public consultation and on the opinion of the BSG

The EBA publicly consulted on the guidelines contained in this paper.

The consultation period lasted for 3 months and ended on 19 June 2015. 57 responses were received, of which 48 were published on the EBA website, including the opinion of the BSG.

This paper presents a summary of the key points and other comments arising from the consultation, the analysis and discussion triggered by these comments and the actions taken to address them if deemed necessary.

In many cases, several industry bodies made similar comments or the same body repeated its comments in response to different questions. In such cases, the comments, and the EBA's analysis, are included in the section of this paper where the EBA considers them most appropriate.

Changes to the guidelines have been incorporated as a result of the responses received during the public consultation.

Summary of key issues and the EBA's response

Most respondents focused their feedback on the proposed scope of the guidelines and the proposed definition for 'shadow banking entities' and argued for further exemptions. The EBA has carefully considered this feedback and amended the definition of 'excluded entities' to consider additional exceptions, which were intended but not clearly set out in the consultation paper, and has also revised its policy decisions regarding the treatment of certain funds.

Some respondents were critical about the fallback approach, in particular Option 1 in the consultation paper. The EBA has considered this feedback and redesigned the fallback approach along the lines of Option 2 in the consultation paper. The data collection has provided useful input to confirm the calibration of the fallback approach.



Summary of responses to the consultation and the EBA's analysis

Summary of responses received

EBA analysis

Amendments to the proposals

General comments

The EBA's mandate expressly requires that 'international level' developments on shadow banking should be taken into account in the development of these guidelines. Proper coordination has to be ensured with existing international work on shadow banking before setting a definition (e.g. work undertaken by the Basel Committee on Banking supervision, the Financial Stability Board, ESMA or the G20).

There is a need for development of a fundamental and robust level 1 regulation designed for shadow banking entities.

The EBA has given due consideration to on-going work in the area of shadow banking in the Union and other international fora. The EBA has also consulted the ESMA, the FSB, the European Commission services and the European Central Bank regarding the proposed definition of 'shadow banking entities' and has considered their feedback when finalising the guidelines.

The EBA notes that the suggestion for regulating the shadow banking sector goes beyond the scope of the guidelines.

No amendment.

Responses to questions in Consultation Paper EBA/CP/2015/06

Q1. Do you agree with the approach the EBA has proposed for the purposes of defining shadow banking entities?

In particular:

Do you consider that this approach is workable in practice? If not, please explain why and present possible alternatives.

Do you agree with the proposed approach to the exclusion of certain undertakings, including the approach to the treatment of funds? In particular, do you see any risks stemming from the exclusion of non-MMF UCITS given the size of the industry? If you do not agree with the



Summary of responses received	EBA analysis	Amendments to the proposals
<p>proposed approach, please explain why not and present the rationale for the alternative approach(es) (e.g. on the basis of specific prudential requirements, redemption limits, maximum liquidity mismatch and leverage, etc.).</p>		
<p>Most respondents focused their feedback on the scope of the guidelines and the proposed definition of ‘shadow banking entities’.</p>	<p>Definition of ‘credit intermediation activities’</p> <p><i>Portfolio management and advice:</i></p> <p>On reflection, the EBA regards it as inappropriate to include this activity in the list of activities which institutions can consider automatically as ‘credit intermediation activities’, as it is not always the case that this activity will involve credit intermediation. Instead, the institution would need to carry out a case-by-case assessment of an entity’s business (assuming that the entity concerned does not carry out one of the other activities listed in the definition of ‘credit intermediation activities’) in order to identify whether the entity is to be considered a ‘shadow banking entity’ for the purposes of the guidelines.</p>	<p>Definition of ‘credit intermediation activities’</p> <p><i>Portfolio management and advice:</i></p> <p>The definition of ‘credit intermediation activities’ has been amended to omit the reference to point 11 of Annex I to the CRD (portfolio management and advice).</p>
<p>Definition of ‘credit intermediation activities’:</p> <ul style="list-style-type: none"> • Portfolio management and advice – regarding the definition of ‘credit intermediation activities’, feedback noted that ‘credit intermediation activities’ are not present while carrying out portfolio management and advice according to point 11 of Annex I of the CRD. Moreover, this activity is also regulated by the Markets in Financial Instruments Directive 2004/39/EC, by the UCITS Directive and, if undertaken by AIF managers, the AIFMD. • Relation of bank-like activities and CRD/Annex I references - some respondents also sought clarification of whether the four proposed bank-like activities for the identification of an activity as ‘credit intermediation activities’ are independent of the eight activities proposed by reference to Annex I of CRD IV. 	<p><i>Relation of bank-like activities and CRD/Annex I references:</i></p> <p>The referenced activities mentioned in Annex I of the CRD should be understood as examples</p>	<p><i>Relation of bank-like activities and CRD/Annex I</i></p>
<p>Definition of ‘excluded undertaking’:</p> <p>Broadly, respondents’ view was that the proposed catalogue of excluded undertakings is too narrow, and does not take into account the wide diversity in underlying business models and activities that exists in practice. Various additional segments of the non-bank sector should be excluded from the definition of ‘shadow banking entities’. Respondents</p>		



Summary of responses received

cited the existence of various regulatory frameworks that applied already to certain entities in the non-bank sector. Concerns on the impact of the proposed broad scope were expressed – including about the cost of financing to the real economy in some cases. A list of the entities that were put forward for exclusion by respondents (in addition to those identified in the EBA’s proposed list of excluded undertakings) is provided below. Some respondents proposed that the EBA use the definition of ‘unregulated financial entity’ as set out in Article 142(1) point 5 of Regulation (EU) No 575/2013 (the CRR).

- **Money market funds (MMFs)** – respondents noted that most MMFs in the EU (80% of the assets and 60% of the funds) operate under the rules of the UCITS Directive⁴⁴, with the remainder operating (since July 2013) under the rules of the AIFMD⁴⁵. Respondents cited the following requirements as providing specific prudential controls:
 - i) Run risk and/or liquidity problems are addressed by risk management, liquidity management requirements, gates and liquidity fees requirements as set out in Article 16 of the AIFMD and Section 4 of Regulation 231/2013⁴⁶, and/or

EBA analysis

of credit intermediation activities.

Definition of ‘excluded undertaking’

MMFs:

The EBA notes the consultation feedback regarding MMFs.

For the reasons given in the consultation paper the EBA considers that, at this stage, in particular pending the agreement of the European Commission’s proposal for a regulation on MMFs⁶¹, and noting the size of the funds (for instance, relative to other types of UCITS), it remains appropriate for MMFs to fall within the scope of the definition of ‘shadow banking entity’. The EBA will keep the scope of the guidelines under review, in particular having regard to relevant regulatory

Amendments to the proposals

references:

No amendment.

Definition of ‘excluded undertaking’

MMFs:

No amendment.

AIFs:

The definition of ‘excluded undertaking’, point K) has been amended.

⁴⁴ Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS).

⁴⁵ Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010.

⁴⁶ Commission Delegated Regulation (EU) No 231/2013 of 19 December 2012 supplementing Directive 2011/61/EU of the European Parliament and of the Council with regard to exemptions, general operating conditions, depositaries, leverage, transparency and supervision.



Summary of responses received	EBA analysis	Amendments to the proposals
<p>Directive 2010/43/EU⁴⁷, as well as more MMF-specific requirements by CESR guidelines 10-49⁴⁸ and ESMA guidelines, which since 2010 have imposed strict limits in term of liquidity, risk and leverage on all MMFs in Europe and limit the use of derivatives.</p> <p>ii) Interconnectivity and spillovers are addressed by counterparty limits and risk management requirements as set out in Article 15 of AIFMD and Section 3 of Regulation 231/2013, the UCITS Directive and Directive 2010/43/EU.</p> <p>iii) Excessive leverage and procyclicality are addressed by limits on leverage and disclosure on leverage as set out in Articles 11, 22 and 112 of the AIFMD, the UCITS Directive, Directive 2010/43/EU and CESR guidelines 10-788⁴⁹, as well as more MMF-specific requirements by CESR guidelines 10-49 and ESMA guidelines 2014/110.</p> <p>iv) Opaqueness and complexity are addressed by the obligation</p>	<p>developments.</p> <p><i>AIFs:</i></p> <p>The EBA has considered the feedback received during the consultation period as well as input from ESMA and the European Commission. The EBA acknowledges that AIFs are regulated indirectly, as a result of requirements imposed on their asset managers under the AIFMD. However, the risks arising directly from the funds themselves are not mitigated in a satisfactory way from a prudential point of view. For example, while leverage is strictly limited for UCITS funds, a similar limitation does not apply to AIFs. Given this, the EBA is of the view that only AIFs with limited leverage could be considered to fall outside the definition of ‘shadow banking entities’. Under the AIFMD, a</p>	<p><i>Particular case of EuVECAs, EuSEFs and ELTIFs:</i></p> <p>The definition of ‘excluded undertaking’, point K) has been amended to include these specific cases.</p> <p><i>Transactions with underlying assets:</i></p> <p>No amendment.</p> <p><i>Securitisation</i></p>

⁶¹ The Commission’s proposal is available here: http://ec.europa.eu/finance/investment/money-market-funds/index_en.htm.

⁴⁷ Commission Directive 2010/43/EU of 1 July 2010 implementing Directive 2009/65/EC of the European Parliament and of the Council as regards organisational requirements, conflicts of interest, conduct of business, risk management and content of the agreement between a depositary and a management company.

⁴⁸ CESR’s Guidelines on a common definition of European money market funds (review).

⁴⁹ CESR’s Guidelines on a common definition of European money market funds.



Summary of responses received

to report to investors and regulators (i.e. national competent authorities, ESMA and the ESRB) and supervise managers, as set out by Articles 22, 23, 24, 26, and Annex IV of the AIFMD, and by Commission Regulation (EU) No 583/2010⁵⁰.

Specific existing arrangements under the CRR (e.g. increases in risk weights for institutions' exposures to the unregulated financial sector, higher capital requirements for banks' investments in the equity of funds), as well as the introduction of liquidity and funding requirements under Basel III (e.g. liquidity coverage ratio, net stable funding ratio) were also invoked to prove that institutions will be less susceptible to liquidity and funding risks arising.

The proposed MMFs Regulation⁵¹ was noted, which will soon add to the weight of regulation on this sector. Further, the importance of MMFs as a source of funding for governments, corporates and financial institutions was highlighted – with concerns raised on how the guidelines may affect MMFs' role in providing this finance.

- **Alternative investment funds (AIFs)** – respondents noted that all non-UCITS investment funds are regulated under AIFMD – which applies similar or even identical requirements to UCITS in many areas, e.g. liquidity management requirements, counterparty limits, leverage restrictions and disclosure. Respondents cited the following

EBA analysis

fund manager who manages an AIF which employs leverage must, on a regular basis, disclose to its investors any change to the maximum level of leverage permitted as well as any re-hypothecation rights or any guarantee granted under the leveraging arrangement and the total amount of leverage employed by the AIF. For an institution, it would thus be easy to identify which AIF counterparty is leveraged or not.

In addition to this condition, only AIFs which are not allowed to originate loans or purchase third parties' lending exposures and add them to their balance sheets would be excluded from the definition of 'shadow banking entity'.

Particular case of EuVECAs, EuSEFs and ELTIFs:

Regarding the particular case of EuVECAs (European Venture Capital Funds), EuSEFs (European Social Entrepreneurship Funds) and ELTIFs (European Long Term Investment Funds), the EBA is of the view that since these funds are

Amendments to the proposals

activity:

No amendment.

Factoring and leasing companies:

The definition of 'financial institution' has been amended to clarify that it is to be interpreted in line with Article 119(5) of the CRR.

Payment institutions and electronic money issuers:

The definition of

⁵⁰ Commission Regulation (EU) No 583/2010 of 1 July 2010 on key investor information and conditions to be met when providing key investor information or the prospectus in a durable medium other than paper or by means of a website.

⁵¹ The Commission's proposal for the regulation is available here: http://ec.europa.eu/finance/investment/money-market-funds/index_en.htm.



Summary of responses received

EBA analysis

Amendments to the proposals

requirements as providing specific prudential controls:

- i) Run risk and/or liquidity problems are addressed by risk management, liquidity management requirements, gates and liquidity fees requirements as set out by Article 16 of the AIFMD, Section 4 of Regulation 231/2013 and the EVCA risk measurement guidelines⁵².
- ii) Interconnectivity and spillovers are addressed by counterparty limits and risk management requirements as set out by Article 15 of the AIFMD and Section 3 of Regulation 231/2013.
- iii) Excessive leverage and procyclicality are addressed by limits on leverage and disclosure on leverage as set out in Articles 11, 22 and 112 of the AIFMD.
- iv) Opaqueness and complexity are addressed by the obligation to report to investors, report frequently and in a granular way to regulators (i.e. national competent authorities, ESMA and the ESRB) and supervise managers, as set out by Articles 22, 23, 24, 26, and Annex IV of the AIFMD.

It was stressed that supervisory reporting on a quarterly basis is mandatory for most AIFs and includes detailed information on portfolio composition, principal exposures and most

closed-ended vehicles that do not usually perform credit intermediation they should fall outside the definition of 'shadow banking entity' and be out of the scope of the guidelines.

Transactions with underlying assets:

The EBA notes that the guidelines apply in parallel with Commission Delegated Regulation (EU) No 1187/2014 of 2 October 2014. This delegated regulation addresses concerns related to the failure of a single counterparty or a group of connected counterparties and sets out conditions under which the transaction itself does not constitute an additional exposure and is not subject to a limit. The guidelines address a different set of concerns, as laid out in the background section, and require that any transaction is subject to a limit.

Securitisation activity:

The mere fact that a securitisation is compliant

'excluded undertaking' has been amended to include two new points dealing expressly with 'electronic money institutions' and 'payment institutions'.

Resolution authorities, bridge institutions and asset management vehicles and similar entities established for the purposes relating to the resolution of institutions:

The definition of 'excluded

⁵² <https://www.evca.eu/media/10083/EVCA-Risk-Measurement-Guidelines-January-2013.pdf>



Summary of responses received	EBA analysis	Amendments to the proposals
<p>significant counterparty concentrations, risk profile and liquidity management, which proves helpful for assessing the interconnectedness between institutions and other financial entities. Furthermore the AIFMD reporting has been developed with the specific aim of enabling supervisory authorities to effectively monitor systemic risks associated with AIF management. Specific reporting is due by AIFs that use significant leverage (commitment in excess of 3 for 1 of capital).</p> <p>v) An exchange of information on the potential systemic consequences of AIFM activity is ensured by Article 116 of the AIFMD.</p> <p>vi) The obligatory use of AIF depositaries means that legal and operational structures must be provided to prevent cash flows from being redirected, just as with UCITS.</p> <p>The proposed Securities and Financing Transactions Regulation⁵³, Solvency II, and the Banking Structural Reform Regulation⁵⁴ were cited as a further set of requirements that will soon add to the weight of regulation on AIFs and the interactions between credit institutions and AIFs.</p>	<p>with the ‘Simple, transparent and standardised’ (STS) requirements would not be sufficient to justify securitisation vehicles being ‘excluded undertakings’. In fact, the STS requirements do not mitigate prudential risk as such. Nevertheless the institution could take into account the fact that a securitisation is compliant with STS requirements when setting up a limit to its individual exposure to such securitisation.</p> <p><i>Factoring and leasing companies:</i></p> <p>The feedback touches two different aspects. Firstly, the industry claims that there is low reliance on short-term funding amongst leasing companies. This point relates to the question whether the criteria of ‘credit intermediation activity’ are fulfilled or not (see above). The EBA notes in this regard that this statement needs to be taken into account while applying the guidelines. It does not request a modification of</p>	<p>undertaking’ has been amended to include a new point for such entities.</p> <p><i>Financial companies carrying out credit intermediation activities for group companies:</i></p> <p>The definition of ‘excluded undertaking’ has been amended to include a new point (o) to cover entities which have as their principal activity</p>

⁵³ The Commission’s original proposal for the regulation is available here: http://ec.europa.eu/finance/general-policy/shadow-banking/index_en.htm#maincontentSec1.

⁵⁴ The Commission’s original proposal for the regulation is available here: http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CC0QFjAB&url=http%3A%2F%2Feur-lex.europa.eu%2Flegal-content%2FEN%2FALL%2F%3Furi%3DCELEX%3A52014PC0043&ei=V6CSVYD_JcOX7Qan8JH4Cw&usq=AFQjCNHS6W7SrEYm95rX6F12fm86uF38RA&bvm=bv.96783405,d.ZGU.



Summary of responses received

A number of bodies also stressed that the population of AIFs is very diverse – and that the draft guidelines risked applying an inappropriate ‘one size fits all’ approach that would ignore the divergent riskiness that different AIFs represent. In this same regard, some respondents suggested that only AIFs that employ substantial leverage (as defined in Article 111 of Regulation 213/2013) should be captured in the guidelines.

The distinction that has been proposed between AIFs and UCITS was also questioned – as some respondents stated that AIFs are often not substantially different from UCITS in risk terms, or in terms of the prudential regime applied. Furthermore the treatment of non-UCITS (and MMFs) should be consistent throughout the large exposure framework, in particular considering Commission Delegated Act 1187/2014⁵⁵, which distinguishes funds solely based upon their added risk.

Most respondents see no specific justification for not excluding from the scope of the term ‘shadow banking entity’ certain closed-ended and unleveraged AIFs, EuVECAs, EuSEFs and ELTIFs, as these provide useful and much-needed financing to EU businesses and economies.

- **Transactions with underlying assets** – some respondents highlighted a risk of duplication in cases where institutions ‘look through’⁵⁶ their

EBA analysis

‘credit intermediation activity’.

Secondly, assuming that a specific leasing or factoring company exercises ‘credit intermediation activity’, these companies will fall within the definition of ‘financial institution’ according to point (e) of excluded undertakings. The EBA clarifies that the definition of ‘financial institution’ should be interpreted in line with Article 119(5) of the CRR (exposures to institutions). That is, where an institution’s exposure to an entity (for instance a factoring or leasing company) is treated as an exposure to an institution pursuant to Article 119(5) of the CRR, because the entity is subject to a comparable prudential framework to that applicable to institutions in terms of robustness, the entity should be regarded as a ‘financial institution’ for the purposes of the guidelines. In such cases the entity shall not be treated as a ‘shadow banking entity’ for the purposes of the guidelines.

Amendments to the proposals

carrying out credit intermediation activities for their parent undertakings, for their subsidiaries or for other subsidiaries of their parent undertakings.

Consolidation

No amendment.

Equivalence of third country regimes

No amendment.

⁵⁵ Commission Delegated Regulation (EU) No 1187/2014 of 2 October 2014 supplementing Regulation (EU) No 575/2013 of the European Parliament and of the Council as regards regulatory technical standards for determining the overall exposure to a client or a group of connected clients in respect of transactions with underlying assets.

⁵⁶ See Article 7 of Commission Delegated Regulation (EU) No 1187/2014 - banks can base their exposure for the purposes of the large exposures regime solely on the assets in the funds and do not have to include the funds themselves or their managers.



Summary of responses received

exposures to investment funds in measuring their exposures for large exposures purposes. Where the look-through approach is used for measuring exposures to a fund (e.g. UCITs and AIFs), it was argued that additional exposure limits under the proposed guidelines are not necessary – and thus that the exposure to the fund should be excluded from the scope of the guidelines.

- **Securitisation activity** – Related to the *Look-Through Approach*, some respondents noted that exposures to securitisations are also generally handled under this system – and thus that exposures arising in connection with securitisations should also be explicitly excluded from the scope of the guidelines. Additionally, some concerns were expressed that capturing securitisation exposures would run counter to the overall direction of policy at present, which is seeking ways to ‘revitalise’ securitisation markets. Such concerns applied also to special-purpose vehicles (SPVs) and conduits, which respondents argued should also be excluded from the guidelines. Traditional ‘self-liquidating’ securitisation activity, it was argued, does not involve material maturity transformation, as investors’ rights to repayment arise from the cash generated by the underlying securitised assets. Given this, securitisation activity may not involve ‘bank-like activity’ and thus it should be made explicit that this situation is excluded from the definition of shadow banking for the purpose of these guidelines. Where securitisations meet the new requirements (to be finalised) for *simple, transparent, and standardised* securitisation, the above

EBA analysis

Payment institutions and e-money issuers:

The EBA agrees that, due to the Union frameworks applicable to such entities, the definition of ‘excluded undertaking’ should be clarified to make it clear that such entities are not to be treated as a ‘shadow banking entity’ for the purposes of the guidelines. The EBA also points out that this clarifies a pre-existing policy position.

Resolution authorities, bridge institutions and asset management vehicles and similar entities established for the purposes relating to the resolution of institutions:

The EBA agrees with the consultation feedback regarding the treatment of exposures to entities established for purposes relating to the resolution of institutions pursuant to Directive 2014/59/EU or for similar purposes as, broadly speaking, these entities are established in pursuance of public policy objectives relating to financial stability. Accordingly the EBA agrees that such entities should not fall within the scope of the definition of ‘shadow banking

Amendments to the proposals

Groups of connected clients

The definition of ‘exposure to shadow banking entity’ has been amended to clarify that these are exposures to individual entities.



Summary of responses received

arguments for exclusion were felt to be stronger still. Additional relevant prudential requirements in relation to securitisation were also noted – including within the CRR, where specifics are laid out on minimum retention, the treatment of liquidity lines to SPVs and the risk weighting of credit exposures⁵⁷.

- **Factoring and leasing companies** – feedback from the industry noted that this sector is regulated under national law⁵⁸, and thus is subject to some prudential requirements that ensure risks are appropriately managed. Given this, some respondents advocated for the exclusion of this sector from the scope of the guidelines. Further, it was claimed that the activity in this sector is not generally ‘banking-like’ – and therefore it would not be appropriate for the sector to be labelled as ‘shadow banking’. In particular, it is claimed that there is low reliance on short-term funding amongst these companies, that leverage is not a major feature of the markets they operate in and that they are generally transparent – e.g. via published accounts of parent companies. The statement by the Haut Conseil de Stabilité Financière

EBA analysis

entity’.

Financial companies carrying out credit intermediation activities exclusively for group companies:

The EBA notes the consultation feedback regarding the treatment of entities which carry out credit intermediation activities exclusively (or as their main business) for non-financial sector group companies. The EBA agrees that such entities should not fall within the scope of the definition of ‘shadow banking entity’ as long as their principal activity is to carry out credit intermediation activities for other entities of their non-financial group and not for third parties.

Consolidation

Amendments to the proposals

⁵⁷ See Part 3, Chapter 5, and Part 5 of the CRR.

⁵⁸ For example, the feedback noted national regimes in (i) supervision by the German supervisory authority for financial services institutions and the Deutsche Bundesbank that are legally enabled by the German Banking Act to obtain a comprehensive assessment of the risk situation of any leasing company at any time, (ii) UK Financial Conduct Authority’s regime regulating the consumer credit markets and (iii) authorisation and regulation by the French national competent authority.



Summary of responses received

EBA analysis

Amendments to the proposals

(HCSF) in its 2015 annual report that French financing companies do not constitute shadow banks was noted⁵⁹. It was also suggested that it should be clarified that rental companies are not considered leasing companies.

- **Payment institutions and electronic money institutions** – their exclusion should be clarified, as such institutions are regulated and authorised under the EU Payment Services Directive 2007/64 (PSD-1) and EU E-money Directive 2009/110, and also, if credit related to payment services is granted, under Article 16, paragraph 3, of the PSD-1.
- **Public resolution agencies** ('Finanzmarktstabilisierungsfonds') – these institutions wind down risk exposures and non-strategic business lines from banking institutions in trouble. They are subject to German national legislation⁶⁰ and supervision by the German Federal Agency for Financial Market Stabilisation and the German Federal Financial Supervisory Authority.
- **Finance companies relating to industrial groups** – concerns were expressed that the proposed approach would capture exposures to entities that carry out 'bank-like activities' only as a small part of their business, e.g. the treasury/liquidity management function of

The EBA's intention is to exclude entities which are subject to prudential consolidation (i.e. which form a group with an institution) and to which CRR/CRD requirements apply at the consolidated level.

Equivalence of third country regimes

The EBA notes the consultation feedback regarding the process for assessing the equivalence of third country regimes. The EBA notes that this is a cross-cutting issue relevant to the application of various provisions of the CRD/CRR which refer to entities subject to third country regimes comparable to those in the Union. Consistent with normal practices, it is for institutions to assess whether a third country regime is comparable. In so doing, institutions may have regard to relevant decisions, including the Commission's Decision of 12 December 2014 on the equivalence of the supervisory and regulatory requirements of certain third countries and territories for the purposes of the treatment of exposures

⁵⁹ http://www.economie.gouv.fr/files/hcsf_rapport_annuel_062015.pdf

⁶⁰ Act on the Establishment of a Financial Market Stabilisation Fund (Finanzmarktstabilisierungsfonds Gesetz, FMStFG).



Summary of responses received

corporates. It was considered disproportionate to capture the exposure within the guidelines, as such intragroup operations are industry standard practices and neither create additional risks for the group as a whole nor increase the interconnectedness with institutions and the financial system (and thus do not pose a systemic risk). EMIR exempts intragroup OTC derivative transactions from the clearing obligation and margining requirements for non-centrally cleared transactions as long as the clearing thresholds are not crossed. In the same way, Article 2(1)(b) of Directive 2014/65/EU (MiFID II) deliberately waives the application of its provisions in full with regard to investment services exclusively provided for parent undertakings, for subsidiaries or for other subsidiaries of the parent undertaking. The EU legislature also recognises that (i) transactions in derivatives which are objectively measurable as reducing risks directly relating to the commercial activity or treasury financing activity and (ii) intragroup transactions that serve group-wide liquidity or risk management purposes shall not be considered when determining the extent to which ancillary activities constitute a minority of activities at a group level for MiFID II purposes (see Article 2(4), fifth subparagraph, of MiFID II).

To address this point, some respondents proposed that only entities that carry out banking activity as their *main* business should be

EBA analysis

according to Regulation (EU) No 575/2013 of the European Parliament and of the Council⁶², and any relevant assessments of relevant authorities in the Member State in which the institution concerned is established and other relevant materials. In line with normal supervisory practices, competent authorities will be able to challenge the assessment of institutions as to the comparability of third country regimes.

Groups of connected clients

The EBA clarifies that these guidelines only apply to exposures to individual counterparties, i.e. individual shadow banking entities, and do not require the creation of groups of connected clients.

The large exposures regime, as set out in Regulation (EU) No 575/2013, applies independently of these guidelines.

Amendments to the proposals

⁶² The Commission's decision is available here: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.359.01.0155.01.ENG.



Summary of responses received

EBA analysis

Amendments to the proposals

captured by the guidelines. As an alternative, other respondents proposed that the *de minimis* exposure amount should be increased from 0.25% of a bank's capital to either 1% or €300m.

Consolidation:

Respondents supported the approach of excluding entities that are consolidated on an institution's balance sheet. It should be clarified that this applies also for entities consolidated on a voluntary basis, or entities that are subject to mandatory prudential consolidation under the CRR but are excluded from the scope of prudential consolidation on the basis of Article 19 of the CRR.

Equivalence of third country regimes:

In addition to scope issues, further clarity was sought on how the guidelines would work in practice in some areas. Most prominently, respondents noted a lack of clarity on how to judge whether a third country's prudential/regulatory requirements are 'equivalent' or 'comparable' to those applied under Union law. Respondents supported an approach that would allow institutions to make their own equivalence/comparability assessments – subject to ex post review of those assessments by the authorities. This is seen as advantageous, as it would avoid delays associated with centralised equivalence decisions. At a minimum, further details were requested on how equivalence decisions would be taken forward by authorities. The importance of this issue was seen as particularly high in the area of the requirements for credit institutions and insurers. In such cases, few equivalence decisions have yet been taken by the Commission – and thus exposures to banks or insurers in many third countries may unnecessarily fall into the scope of the



Summary of responses received

EBA analysis

Amendments to the proposals

guidelines unless a practical solution is identified. One respondent queried whether an insurance company in a third country not considered to have an equivalent regime would be considered within the scope of the guidelines.

Groups of connected clients:

Finally, it remained unclear to some respondents how the guidelines would apply to groups of connected clients (GCCs). Further details were requested to explain (i) whether the guidelines would apply only to an entity within a GCC that met the relevant shadow banking definition, or whether the guidelines would instead capture the entire GCC as a single exposure, and (ii) the procedure to adopt in case of a classification of the parent company as an unregulated financial entity pursuant to Q&A 2013_492.

Q2. Do you agree with the approach the EBA has proposed for the purposes of establishing effective processes and control mechanisms? If not, please explain why and present possible alternatives.

{30 out of 57 respondents were silent on this question}

According to a minority (4) of the respondents, this question should not be addressed at this stage, as establishing processes and control mechanisms is only possible once the scope of exposures under review has been clearly defined, or a full impact assessment has been conducted.

Several of the respondents (8) broadly agree with the approach taken in allowing institutions to rely on their own internal framework and risk

The EBA notes the broad support for the guidelines' approach regarding the setting up of internal limits by the institutions. No amendment.

The EBA also notes the comments on the need to apply the guidelines in a proportional way. However, the EBA is of the view that risks posed by exposures to shadow banking entities need



Summary of responses received

appetite to set internal limits.

There is, however, also a substantial call (9) to introduce a principle of proportionality. This is justified because (i) the scope is so broad as to encompass entities which are very different in nature and not exposed to the same increased risks and (ii) the requirement to ‘identify all potential risks [...] and the potential impact of those risks’ is relatively broad and will result in operational challenges. According to their views, some exposures warrant very high levels of due diligence, whereas other exposures could easily be demonstrated to be less risky and less complex. The intensity and frequency of monitoring carried out should vary accordingly.

Some respondents (4) stressed that it is important that the requirement for establishing effective process and effective mechanisms should be applied on a consolidated basis only, as:

- Large exposure limits under CRR rules already apply at both solo and consolidated levels and so a sufficient backstop already exists within the current framework.
- Applying the guidelines at consolidated level only would make it easier for institutions to manage the requirements within the ICAAP process, as individual legal entities may have only a partial view of the phenomenon.
- The burden of infrastructure, systems and processes that institutions would need to put in place to comply with the guidelines would be kept proportionate.

EBA analysis

to be monitored and managed regardless of the size, complexity or business model of the institution. The fact that institutions are allowed to set up internal limits as part of their risk assessment processes should ensure an application of the guidelines which is adequate to the institutions’ risk profile.

The EBA clarifies that these guidelines do not intend to introduce additional Pillar 2 requirements, but that the assessments should be done in the context of the regular Pillar 2 assessments, but with a focus on the shadow banking sector as a specific exposure class.

Amendments to the proposals



Summary of responses received

EBA analysis

Amendments to the proposals

Some respondents (3) oppose aggregating limits, as they do not consider the targeted risk to be sectoral. It would be excessive to assume that shadow banking entities by their very nature have a default correlation close to one and thus pose a high concentration risk. Shadow banking entities are subject to (i) individual large exposure limits, (ii) a look-through approach to the ultimate underlying assets of a transaction and (iii) the limitation of exposures to individual counterparties or groups of connected clients under the current large exposure framework of the CRR. Some respondents therefore argued that an aggregate limit would give few additional benefits over the current framework. The targeted risk could be better addressed via ICAAP/Pillar 2, which specifically covers concentration risk, rather than the large exposure regime, which is intended to address default of single entities or groups of connected counterparties.

It was requested that EBA clarify whether it wishes to introduce additional Pillar 2 requirements or whether compliance with the existing framework is sufficient, and whether the look-through requirements should be considered or not for the definition of the exposure. The assessment of the performed analyses could also be made consistent with the internal authorisation levels in the credit process.

Some respondents (4) saw no issues of substance that would justify introducing additional specific Pillar II requirements relating to shadow bank exposures.

In their opinion, requirements for institutions' risk management (credit risk, market risk, operational risk, etc.) are already sufficient to address shadow banking issues. Moreover, the use of Pillar 2 measures in such a



Summary of responses received

EBA analysis

Amendments to the proposals

complex context might result in very heterogeneous implementation, thus endangering the level playing field among banks operating across borders. Furthermore the requirements regarding effective processes and control mechanisms, and oversight by the management body of the institutions as set out in the draft guidelines, would cause unnecessary additional administrative effort with few corresponding benefits.

Q3. Do you agree with the approach the EBA has proposed for the purposes of establishing appropriate oversight arrangements?

{37 out of 57 respondents were silent on this question}

A significant number (8) of the respondents to this question share the EBA's view on the approach to oversight arrangements. This supports the view that institutions' management bodies must review and approve their shadow banking risk appetite and related risk management processes.

Some respondents emphasised that attention should be paid to avoid duplication of work which would create additional burdens and overlaps. A minority of the respondents (3) explicitly opposed the idea of introducing separate qualitative requirements for exposures to shadow banks that are already part of Pillar II processes (e.g. internal risk management, governance of the institutions). These respondents do not see the need to add a specific layer for these broad bases of entities, as risk weighting criteria already exist for many of the transactions performed with clients/debtors or counterparties. One respondent even added that imposing such requirements is not covered by the mandate under Article 395(2) of the CRR.

The EBA notes the broad support for its proposals.

The EBA agrees with the suggestion that the institution's management body could delegate certain reviews to senior management.

Amendment to the section on oversight by the management body of the institution.



Summary of responses received

EBA analysis

Amendments to the proposals

Another theme was that shadow banking entities should not be considered a single risk category. This could lead to underestimating risk for the risky exposures and over-allocation of risk management resources to the less risky exposures. Proportionality should be introduced taking into account the size, riskiness and nature of the exposures concerned.

On a more practical side, it was also highlighted that the management body should be allowed to delegate necessary reviews to specialised and more relevant employees, such as the Chief Risk Officer and Risk Control function. Furthermore, sufficient time should be granted for the operationalisation of these requirements, e.g. via a phased implementation approach to avoid potential macrosystemic risks if banks are not in a position to use the principal approach on 1 January 2016.

According to two respondents (2), it seems inappropriate to establish oversight arrangements before finalising a clear narrow definition of a shadow banking entity. Taking together a wide variety of vehicles may result in a very heterogeneous portfolio, the constituents of which are highly unlikely to impact an institution at the same time or in the same way. It seems unclear to these respondents how a bank would set a strategy and define a risk appetite for such a diverse group of exposures. Further, as the oversight arrangements cover such a wide array of exposures, it might distract the risk management's resources from the most risky ones. A full impact analysis is also requested, to show whether the sectoral definition applied for the aggregation under the shadow bank definition will result in a population which behaves in a correlated fashion.

Q4. Do you agree with the approaches the EBA has proposed for the purposes of establishing aggregate and individual limits?



Summary of responses received

EBA analysis

Amendments to the proposals

{31 out of 57 respondents were silent on this question}

Some respondents (5) agreed in principle with the proposed approach and welcomed the principle of proportionality reflected within it. Opponents (7) claimed that no risk management benefits would be generated by the guidelines, as banks' routine lending processes and strategies for managing credit risk are already sufficiently robust. The approach was also criticised for potentially working against the objectives of Capital Market Union.

Whereas a few (2) suggest having a limit at the aggregate level, most of the respondents (8) have significant reservations regarding the requirement for institutions to set an aggregate limit to the entire shadow banking sector. These concerns were particularly based on the heterogeneity of the targeted population, which would make calibration of an objectively 'appropriate' aggregate limit difficult. Individual limits were preferred by these respondents, as they could be calibrated more simply, and would better fit with the philosophy of the large exposure regime⁶³.

Those concerned with the calibration of aggregate limits requested that an impact study be undertaken. Further, they advocated the introduction of the following amendments:

- Reduction of the scope of the guideline so as exclude all UCITS,

The EBA recognises the role the shadow banking sector plays in providing alternative sources of funding to the real economy. Given this, the EBA considers it premature to use the guidelines to introduce a quantitative limit to institutions' individual or aggregated exposures to these shadow banking entities.

The approach described in the guidelines allows institutions to set risk tolerance levels for exposures to shadow banking entities, corresponding to their risk appetite, within their overall business model and risk management framework, with competent authorities retaining the ability to take supervisory measures where appropriate.

This approach places the responsibility on institutions to demonstrate that the risks related to exposures to shadow banking entities are being managed effectively, in particular by improving, where necessary, the due diligence carried out concerning these exposures.

No amendment.

⁶³ The large exposure regime is traditionally designed to act as a backstop to individual client limits rather than to address sectoral credit concentration risk.



Summary of responses received

EBA analysis

Amendments to the proposals

and AIFs without substantial leverage, including VNAV MMFs.

- Preferential treatment of exposures related to central clearing activities.
- Exemption for certain custody-related services.
- Increase of the materiality threshold.

Should the EBA decide to introduce new limits, some respondents advocated either a blanket aggregate limit⁶⁴ or a general individual limit to shadow banking entities of 20% of eligible capital subject to the condition that the definition of shadow banking entities is narrowed. If these alternatives are not considered acceptable and the idea of establishing both individual and aggregate limits is retained, it was considered essential to drop the fallback approach.

The issue was also raised whether the draft guidelines go significantly beyond the CRR mandate in setting out a combination of aggregate and individual limits.

Q5. Do you agree with the fallback approach the EBA has proposed, including the cases in which it should apply? If not, please explain why and present possible alternatives.

Do you think that Option 2 is preferable to Option 1 for the fallback approach? If so, why? In particular:

⁶⁴ For example, at a level of between 500% and 800% of eligible capital.



Summary of responses received

EBA analysis

Amendments to the proposals

Do you believe that Option 2 provides more incentives to gather information about exposures than Option 1?

Do you believe that Option 2 can be more conservative than Option 1? If so, when?

Do you see some practical issues in implementing one option rather than the other?

{34 out of 57 respondents were silent on this question}

A few respondents found it hard to agree or disagree with the fallback approach, as there is no justification as to why the 25% limit would be relevant. Some respondents expressed concern that the proposed fallback approach is unlikely to serve as an effective risk management tool, as it is quite blunt and might ignore the materiality aspect, which is part of every loan decision. Further, the need for a fallback was questioned, given that shortcomings in setting internal credit exposure limits can be addressed under the SREP. In addition, concerns were raised that this approach may run the risk of setting a de facto limit of 25% should banks be unable to meet the data requirements that would enable them to use the principal approach by 1 January 2016. If a fallback approach will be applied, the majority tended to favour Option 2. The following reasons were cited:

- Shadow banking entities will be a very heterogeneous group with different business models, levels of disclosure and risk levels within their portfolios. Based on this heterogeneity, it does not seem appropriate that, if a credit institution gathers all required information for the majority of those entities but, for a small group of entities, cannot obtain the information required to set a

The EBA has given great consideration to the feedback received in the context of the consultation and has changed the design of the fallback option.

The rationale was threefold.

First of all, one of the objectives of the guidelines is to create appropriate incentives for institutions to have in place the right processes and procedures to gather information on shadow banking entities. In this sense, the incapacity of an institution to get information on a minor part (or even on one only) of its exposures to shadow banking entities would de facto hinder the incentives for the 'search for information' also with reference to the other exposures to shadow banking entities.

The EBA has also considered the importance of the coherence between the fallback approach and the concept of the 'unknown client' defined in the delegated regulation regarding the treatment of

The fallback approach has been redefined along the lines of Option 2 in the consultation paper.



Summary of responses received

EBA analysis

Amendments to the proposals

meaningful limits framework, all the bank's exposures to all shadow banking entities - regardless of the information obtained - should be perceived as an exposure to the 'same client' and, as such, will be subject to a 25% aggregate limit.

- Option 2 makes better use of available information and provides stronger incentives to gather information about shadow banking exposures by rewarding the collection and use of pertinent data with appropriate and realistic exposure limits.
- Option 2 is better aligned with the rationale of the large exposure framework to prevent institutions from incurring disproportionately large losses as a result of the failure of an individual client or group of connected clients due to the occurrence of unforeseen events.
- Option 2 is better aligned with the approach of the RTS regarding the treatment of transactions with underlying assets. Here, the 'unknown client' bucket is only required for those exposures for which an institution fails to meet the specific principal requirements of the RTS.
- The Option 2 approach is not unknown outside the area of large exposures, as it applies, for example, to investments in financial sector entities for purposes of capital deductions.
- Option 2 leads to less overestimation of the total population in

exposures to transactions with underlying assets.

Finally, the EBA is aware that a fallback approach based on Option 1 of the consultation paper might not fully respect the proportionality principle, which is one of the crucial elements of EU prudential regulation.

Given the above, therefore, the EBA decided that the fallback approach should be implemented in a way that is coherent with Option 2 of the consultation paper. In particular, the fallback approach will be applied: i) to all exposures to shadow banking entities if institutions cannot meet the requirements regarding effective processes and control mechanisms or oversight by their management board; and ii) if institutions meet the above requirements of processes, control and oversight, only to those exposures to shadow banking entities for which sufficient information is unavailable.

Regarding the calibration, results of the data collection show that a limit of 25% of the institution's eligible capital on aggregate exposures to shadow banking entities would have an impact on around half of the credit institutions and investment firms which reported individual exposures equal or above 0.25% of its eligible capital (i.e. 65 institutions



Summary of responses received

EBA analysis

Amendments to the proposals

case of difficulty eliminating exempt institutions from their datasets.

Option 1 is perceived by some as unnecessarily punitive and not in line with the development of enhanced risk-sensitive regulatory frameworks and internal modelling. In addition it does not provide incentives to develop a robust assessment process, as non-compliance with the principal approach for just one shadow banking exposure will lead to an overall limit to all shadow banking exposures. Furthermore, Option 1 could lead, in the short term, to swift systemic events resulting from the insolvency/fire sale of assets from the shadow banking entities that cannot provide the necessary information to the banking sector. The limit may need to be considerably higher than 25%, as banks may lend up to 25% of their eligible capital to each shadow banking entity with which they do business. A Quantitative Impact Study is requested before such an aggregate limit is set.

Additionally, if the guidelines were to come into force without a suitable grandfathering arrangement, the institutions would be forced to terminate some of their current exposures before the agreed terms, with unforeseeable consequences for the markets.

of the total of 184 institutions that participated in the data collection). However, it should be noted that the results of the data collection are very conservative given that a much wider definition of 'shadow banking entity' was used for purposes of the data collection than the definition used in these guidelines and that the simulations assume that all exposures would be captured by the fallback approach (Option 1 in the consultation paper). It is also noted that the number of individual exposures which are above 25% of the institution's eligible capital is extremely negligible (around 0.01% of all exposures reported). Everything considered and taking into account the risky nature of these exposures, the EBA believes it would be prudentially sound to align the fallback approach with the large exposures limits of 25% of eligible capital (with possible exceptions for positions in the trading book which meet the conditions in Article 395(5) of the CRR and could therefore exceed the 25% limit) to provide a backstop to exposures to counterparties for which the institution is not able to collect sufficient information to set out an internal limit.

Q6. Taking into account, in particular, the fact that the 25% limit is consistent with the current limit in the large exposures framework, do you agree it is an adequate limit for the fallback approach? If not, why?



Summary of responses received

EBA analysis

Amendments to the proposals

What would the impact of such a limit be in the case of Option 1? And in the case of Option 2?

{34 out of the 57 respondents were silent on this question}

Only a few respondents explicitly agree that the 25% limit is an appropriate limit for the fallback approach.

The inclusion of a 'fallback' approach could run the risk of setting a de facto aggregate limit of 25%, as it is unlikely banks will be able to meet the data requirements to allow use of the principal approach from 1 January 2016. This in itself could pose a macrosystemic risk if most or all banks are forced to use the fallback approach from day one. For example, this may spark fire sales, thereby destabilising markets, leading to withdrawal of finance and affecting credit mediation.

The majority of the respondents state that the 25% aggregate limit proposed under the fallback approach is overly conservative and onerous and lacks a robust justification. The assumption of interconnectedness is deemed erroneous and unrealistic. The mere fact that banks gather insufficient information to allow compliance with the specific rules of the principal approach does not imply that all the shadow banking exposures are highly correlated or should be connected. The variety of entities grouped together does not pose a single risk to an institution and should not be understood as the same client. The EBA should refrain from introducing elements related to geographic and sectoral risks that conflict with the existing policy framework for large exposures and the forthcoming framework of the BCBS. A limit of 25% applied sectorally is likely to lead to a need for exposure reductions by institutions, thereby

These guidelines will apply from 01.01.2017, therefore allowing sufficient time for institutions to prepare to meet the data requirements that are required to use the principal approach.

The EBA notes the concerns regarding the 25% aggregate limit (fallback approach) and draws attention to its response to Q5.

The EBA agrees with the consultation feedback pertaining to geographic and sectoral risks and therefore considers it unnecessary to assess exposures via this categorisation.

The EBA has considered the proposed alternative to segment shadow banking exposures and has rejected it, as it is deemed too onerous to implement in practice and would not ultimately ensure a harmonised application of the guidelines and a level playing field and would not allow meaningful comparisons, as each institution may define different segments.

No amendment.



Summary of responses received

EBA analysis

Amendments to the proposals

having a potential impact on the supply of credit to SMEs and hampering growth as well as restraining recent efforts to revive the securitisation market.

As an alternative, some respondents suggest that banks might have the possibility to segment shadow banking exposures between specific sub-groups. Where it is possible to prove that no correlation is observed within a sub-group, individual limits for shadow banking entities should be sufficient - even if the remaining data requirements are not totally fulfilled.

In addition to the main distinction based on the prudential framework, some consider that the criteria of the nature of the activity, the level of risk and the possibility of 'run' effects could be used to introduce granularity in the treatment of shadow banking entities.

If a fallback approach is nevertheless retained, then an appropriate limit, much higher than 25%, would need to be considered. Using the same percentage for an aggregate limit to the whole shadow banking sector as the one currently used for the large exposure limit of Article 395 of the CRR indicates that the proposed percentage is much too low. Reference was made to the aggregate limit for all large exposures (exposures exceeding the 10% threshold) of 800% of own funds in Directive 2006/48/EC (CRD II), a limit in the three-digit range or a whole-number multiplier of an institution's capital base.

