CENTRAL BANK OF CYPRUS

INTERNAL GOVERNANCE OF CREDIT INSTITUTIONS DIRECTIVE OF 2021

This translation is not official.

It has been prepared by the Central Bank of Cyprus to serve as a reference tool.

APRIL 2022*

***(last amended July 2022)**

BUSINESS OF CREDIT INSTITUTIONS LAWS OF 1997 TO (NO. 3) OF 2021

TABLE OF CONTENTS

Directive under sections 19 and 41(1) and (2)

66(I) of 1997
74(I) of 1999
94(I) of 2000
119(I) of 2003
4(I) of 2004
151(I) of 2004
231(I) of 2004
235(I) of 2004
20(I) of 2005
80(I) of 2008
100(I) of 2009
123(I) of 2009
27(I) of 2011
141(I) of 2011
107(I) of 2012
14(I) of 2013
87(I) of 2013
102(I) of 2013
104(I) of 2013
5(I) of 2015
26(I) of 2015
35(I) of 2015
71(I) of 2015
93(I) of 2015
109(I) of 2015
152(I) of 2015
168(I) of 2015
21(I) of 2016
5(I) of 2017
38(I) of 2017
169(I) of 2017
28(I) of 2018
89(I) of 2018
153(I) of 2018
80(I) of 2019
149(I) of 2019
21(I) of 2020
73(I) of 2020
28(I) of 2021
94(I) of 2021
95(I) of 2021.

Official Journal of the EU: L150, 7.6.2019, p. 253

Official Journal of the EU: L176, 27.6.2013, p. 338.

EBA/GL/2021/05 02.07.2021

The Central Bank, exercising the powers conferred on to it in accordance with the provisions of sections 19 and 41 (1) & (2) of the Business of credit institutions Laws of 1997 to (No. 3) of 2021, as well as for the purposes of harmonisation with Directive 2019/878/EU of the European Parliament and of the Council of 20 May 2019 amending Directive 2013/36/EU as regards exempted entities, financial holding companies, mixed financial holding companies, remuneration, supervisory measures and powers and capital conservation measures», and for the renewed harmonisation with Directive 2013/36/EU 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, as well as for the purposes of harmonisation with the EBA guidelines on internal governance, adopts the present Directive.

PART I - TITLE, PURPOSE, SCOPE OF APPLICATION AND DEFINITIONS

Short title.

1.- This Directive shall be cited as the Internal Governance of Credit Institutions Directive of 2021.

Purpose.

2.- This Directive specifies the internal governance arrangements, processes and mechanisms that credit institutions shall implement in accordance with section 19 of the Law, to ensure effective and prudent management of the credit institution.

Scope of application.

3.- (1) This Directive applies in relation to credit institutions' governance arrangements specified in sub-paragraph (2), including their organisational structure and the corresponding lines of responsibility, processes to identify, manage, monitor, and report the risks they have or may undertake, the internal control framework as well as remuneration policies and practices.

(2) This Directive applies to credit institutions based in the Republic, on an individual basis, unless the Central Bank makes use of the derogations as defined in Article 7 of Regulation (EU) No 575/2013. In addition, parent undertakings and subsidiaries subject to this Directive shall –

(a) meet the requirements arising from this Directive on a consolidated or sub- consolidated basis, to ensure that their arrangements, processes, and mechanisms that they maintain are consistent and well-integrated in accordance with the provisions of this Directive and that any data and information relevant to the purpose of supervision can be produced,

(b) implement such arrangements, processes, and mechanisms in their subsidiaries not subject to this Directive, so as to ensure that such arrangements, processes and mechanisms are consistent and well-integrated and that those subsidiaries able to produce any data and information relevant to the purpose of supervision,

(3) The requirements arising from this Directive concerning subsidiaries not subject to the provisions of this Directive, shall not apply if the parent credit institution that is established in the EU or the credit institutions controlled by a parent financing holding company established in the EU or by a parent mixed-activity financing holding company established in the EU, can demonstrate to the Central Bank that the application of this Directive is unconstitutional under the law of the third country where the subsidiary is established.

(4) The provisions of Part 5 shall apply at group, parent, and subsidiary level, including those established in offshore financial centres.

(5) Branches of credit institutions in the Republic authorised in a third country shall be excluded from the scope of application of this Directive.

Definitions.

4.- (1) For the purposes of this Directive, the definitions foreseen by the Law shall apply, unless a different interpretation emerges from the text. In addition, the following definitions shall apply:

6(I) of 2015
93(I) of 2021

«Other systemically important credit institutions» or «O-SII» means the credit institutions as defined in section 6 of the Macroprudential Supervision Law of 2015;

"Chief financial officer" means the person who is overall responsible for managing all of the following activities: financial resources management, financial planning and financial reporting;

R.A.A. 179/2020
O.G. Sch. III(I) No. 5255
29.04.2020
No. 435
18.09.2020

«Independent member of the management body» means the person who is appointed as an independent member upon approval by the competent authority, having met the independence criteria set out in the Assessment of the Suitability of Members of the Management Body and Persons holding Key Positions in Licensed Credit institutions Directives of 2020;

Official Journal of the EU: L176
27.06.2013, p. 1.

«Competent authority» means a competent authority as defined in Article 4 (1)(40) of Regulation 575/2013/EU and/or the European Central Bank for the purpose of carrying out the tasks assigned to it in accordance with Regulation (EU) No 1024/2013;

Official Journal of the EU: L287
29.10.2013, p. 63.

«Risk appetite» means the aggregate level and types of risk a credit institution is willing to assume within its risk capacity, in line with its business model, to achieve its strategic objectives;

«Managing director» means the member of the management body who is responsible for the management and coordination of the overall business activities of a credit institution;

"Outsourcing" means an agreement of any kind between a credit institution and a service provider, by which the service provider carries out a procedure, performs services or activities that would normally be undertaken, provided or exercised by the credit institution itself;

53(I) of 2017
171(I) of 2017
7(I) of 2018
69(I) of 2019
12(I) of 2020

"External auditor" means a third party, independent of the staff of the credit institution or the authorised auditor, appointed for the purposes of auditing the credit institution and who is the statutory auditor and/or statutory audit firm, within the meaning of section 2 of the Auditors Law;

«Head of the internal control function» means the persons at the highest hierarchical level in charge of effectively managing the day-to-day operation of the independent risk management, compliance, internal audit and ICT and security risk management functions;

«Prudential consolidation» means the application of the prudential rules set out in Directive 2013/36/EU and Regulation (EU) No 575/2013 on a consolidated or sub-consolidated basis, in accordance with Part 1, Title 2, Chapter 2 of Regulation (EU) No 575/2013. The prudential consolidation includes all subsidiaries that are credit institutions or financial credit institutions, as defined in Article 4(1)(3) and (26) of Regulation (EU) No 575/2013, respectively, and may also include ancillary services undertakings, as defined in Article 2(18) of that Regulation, established in and outside the EU.

"Internal approaches" means the internal ratings based approach referred to in Article 143 (1) of Regulation (EU) No 575/2013, the internal models approach referred to in Article 221 of Regulation (EU) No 575/2013, the own estimates approach referred to in Article 225 of Regulation (EU) No 575/2013, the advanced measurement approaches referred to in Article 312(2) of Regulation (EU) No 575/2013, the internal model method referred to in Articles 283 and 363 of Regulation (EU) No 575/2013 and the method of the supervisory model referred to in Article 259 (3) of Regulation (EU) No 575/2013;

«Executive member of the management body» means the position of member of the management body where a person is actually responsible for directing the activities of the credit institution through a relevant employment contract concluded with that credit institution;

«Credit institution required to consolidate» means a credit institution that is required to abide by the prudential requirements on the basis of the consolidated situation in accordance with Part One, Title II, Chapter 2 of Regulation (EU) No 575/2013;

«Risk capacity» means the maximum level of risk that a credit institution is able to assume given its capital base, its risk management and control capabilities and its regulatory constraints;

Official Journal of the EU: L158 27.05.2014, p. 77.

«Regulation (EU) No 537/2014» means Regulation (EU) No 537/2014 of the European Parliament and of the Council of 16 April 2014 on specific requirements regarding statutory audit of public-interest entities and repealing Commission Decision 2005/909/EC;

Official Journal of the EU: L203 09.06.2021, p. 1.

«Commission Delegated Regulation (EU) 2021/923» means the Commission Delegated Regulation (EU) 2021/923 of 25 March 2021 supplementing Directive 2013/36/EU of the European Parliament and of the Council with regard to regulatory technical standards setting out the criteria to define managerial responsibility, control functions, material business units and a significant impact on a material business unit's risk profile, and setting out criteria for identifying members of staff or categories of staff whose professional activities have an impact on the credit institution's risk profile that is comparably as material as that of members of staff or categories of staff referred to in Article 92(3) of that Directive;

EBA/GL/2019/02

«ICT and security risk» means risk of loss due to breach of confidentiality, failure of integrity of systems and data, inappropriateness or unavailability of systems and data or inability to change information technology (IT) within a reasonable time and with reasonable costs when the environment or business requirements change. This includes security risks resulting from inadequate or failed internal processes or external events including cyber-attacks or inadequate physical security;

"Model risk" means the potential loss an institution may incur, as a consequence of decisions that could be principally based on the output of internal models, due to errors in the development, implementation or use of such models;

«Risk culture» means a credit institution's norms, attitudes and behaviours related to risk awareness, risk-taking and risk management, and the controls that shape decisions on risks. Risk culture influences the decisions of management and employees during the day-to-day activities and has an impact on the risks they assume;

"Gender pay gap" means the difference between the average annual total gross earnings of men and women expressed as a percentage of the average annual total gross earnings of men;

"Law" means the Business of credit institutions Laws of 1997 to (No. 3) 2021;

"Service provider" means a third-party entity that is undertaking an outsourced process, service or activity, or parts thereof, under an outsourcing arrangement;

«Credit institution» means a credit institution as defined in Article 4(1) of Directive of Regulation (EU) 575/2013;

«Key function holders» means persons who have significant influence over the direction of the credit institution but who are neither members of the management body nor the chief executive officer, and

they include the heads of internal control functions and the chief financial officer, where they are not members of the management body, and, where identified by the credit institution on a risk-based approach; other key function holders might include heads of significant business lines, European Economic Area/European Free Trade Association branches, third country subsidiaries and other internal functions;

Official Journal of the EU.: L176 of 27.6.2013, p. 338.

«Staff» means all employees of a credit institution and its subsidiaries within its scope of consolidation, including subsidiaries not subject to Directive 2013/36/EU, and all members of the management body;

«significant credit institutions» means credit institutions referred to in section 6 of the Macro-prudential Supervision of credit institutions Law of 2015 [global systemically important credit institutions (G-SIIs) and other systemically important credit institutions (O-SIIs)), and, as appropriate, other credit institutions determined by the competent authority or national law, based on an assessment of the credit institutions' size and internal organisation, and the nature, scope and complexity of their activities;

«ICT» means information and communication technology.

The terms "critical operation" and "essential operation" have the same meaning for the purposes of this Directive.

(2) (a) In this Directive, any reference to a Directive, Regulation, Decision or other legislative act of the European Union shall mean that Act as corrected, amended or replaced from time to time, unless otherwise specified in the text.

(b) In this Directive any reference to a law or regulatory administrative act of the Republic, shall mean the said law the regulatory administrative act as corrected, amended or replaced from time to time, unless a different meaning emerges from the text.

PART 2 - PROPORTIONALITY

Proportionality.

5.- (1) The internal governance framework, arrangements, processes and mechanisms, shall be comprehensive and proportionate to the credit institution's nature, scale and complexity of the risks inherent in the business model and activities of the credit institution.

(2) when developing and implementing internal governance arrangements, credit institutions shall take into account their size and internal organisation, and the nature, scale and complexity of their activities. Significant credit institutions shall have more sophisticated governance arrangements, while small and less complex credit institutions may implement simpler governance arrangements. Nevertheless, credit institutions shall be aware that the size or systemic importance of a credit institution may not in itself be indicative of the degree to which the credit institution is exposed to risk.

(3) For the purpose of the application of the principle of proportionality as referred to in sub-paragraph (2), the following criteria shall be taken into account by credit institutions for purposes of application of the requirements of the Directive, as well as by the competent authority for the purpose of assessing the compliance of credit institutions with the requirements of this Directive:

(a) the size in terms of the balance-sheet total of the credit institution and its subsidiaries within the scope of prudential consolidation;

(b) the geographical presence of the credit institution and the size of its operations in each jurisdiction;

(c) the legal form of the credit institution, including whether the credit institution is part of a group and, if so, the proportionality assessment for the group;

(d) whether the credit institution's securities are listed or not in a regulated market;

(e) whether the credit institution is authorised to use internal models for the measurement of capital requirements (for instance, the Internal Ratings Based Approach);

(f) the type of authorised activities and services performed by the credit institution, such as those foreseen by Annex IV of the Law;

(g) the underlying business model and strategy; the nature and complexity of the business activities, and the credit institution's organisational structure;

(h) the risk strategy, risk appetite and actual risk profile of the credit institution, taking into account also the result of the SREP capital and SREP liquidity assessments;

(i) the ownership and funding structure of the credit institution;

(j) the type of clients (for instance, retail, corporate, credit institutional, small businesses, public entities) and the complexity of the products or contracts;

(k) the outsourced activities and distribution channels;

(l) the existing information technology (IT) systems, including continuity systems and outsourcing activities in this area; and

(m) whether the credit institution falls within the definition «small and less complex credit institution» or «Significant credit institution» as defined in points 145 and 146 of Article 4 (1) of Regulation (EU) No 575/2013.

PART 3 – ROLE AND COMPOSITION OF THE MANAGEMENT BODY AND COMMITTEES

Section I – Management body

General requirements.

6.- (1) The management body shall have ultimate and overall responsibility for the credit institution and defines, oversees and is accountable for the implementation of the governance arrangements within the credit institution that ensure effective and prudent management of the credit institution, including segregation of responsibilities and prevention of conflicting interests.

(2) Subject to the provisions of section 19B of the Law, the arrangements referred to in sub-paragraph (1) shall comply with the following principles:

(a) the management body has the overall responsibility for the credit institution and approves and oversees the implementation of the strategic objectives, the risk strategy and the internal governance of the credit institution;

(b) the management body ensures the integrity of accounting and financial reporting systems, including financial and operational controls, and compliance with the relevant law and relevant standards;

(c) the management body oversees the process of disclosures and communications to external stakeholders and competent authorities;

(d) the management body is responsible for the effective supervision of senior management;

(e) subject to the provisions of section 19B (1) of the Law, the chairman of the management body of the credit institution shall not simultaneously exercise the function of a chief executive officer within the same institution;

(f) the members of the management body shall meet the requirements specified in the Appropriateness Assessment of Members of the Management Body and Persons Holding Key Positions in Licensed Credit institutions Directive of 2020;

(g) all of the members of the management body devote sufficient time to the performance of their duties at the credit institution, including the preparation of the meetings of the management body.

(3) For the purposes of point (d) of sub-paragraph (2), the management body shall establish appropriate policies, practices and procedures to ensure that senior management performs their roles and responsibilities in accordance with the provisions of paragraphs 25 to 29.

Practices and procedures shall indicatively include the following:

(a) regular meetings with senior management;

(b) asking questions and critically examining the explanations and information provided by senior management;

(c) setting formal senior management performance targets in line with the credit institution's long-term goals, strategic and financial soundness, and monitoring the performance of senior management in relation to those targets.

(4) (a) Credit institutions shall ensure that data on financial exposures provided to members of the management body and their related parties are properly documented and made available to the competent authority upon request.

(b) For the purposes of this sub-paragraph, the term "related party" shall mean:

184(I)/2015
115(I)/2020

(i) spouse, partner as defined in the Civil Cohabitation Law of 2015, child or parent of a member of the management body,

(ii) a commercial entity in which a member of the management body or a close associate thereof referred to in point (i) has a shareholding of 5% or more of the capital or voting rights in that entity or in which such persons may exercise significant influence or in which such persons hold senior management positions or are members of the management body,

(iii) other natural or legal persons associated with the member of the management body through a relationship of significant influence, exercised either by the member of the management body or by other natural or legal persons.

(c) Among the possible indications of significant influence as referred to in subparagraphs (ii) and (iii) of point (b), which credit institutions shall take into account when conducting their assessment of the existence of interconnection, are those set out in the provisions of point (39) of Article 4 paragraph 1 of Regulation (EU) 575/2013, as well as the following:

(i) Notwithstanding any percentage of participation, each of the following powers of a person who is a member of the management body or of a person who happens to be related to a member of the management body, provides an indication of the exercise of control by that member of the management body in the corresponding entity and therefore the financial exposures of the credit institution towards that entity are included in the financial exposures of that member of the management body:

(A) power to direct the activities of the entity,

(B) power to decide on the entity's significant transactions such as the transfer of profits or losses,

(C) power to appoint or remove the majority of members of the entity's management body,

(D) voting power in meetings of the board of directors, general meetings or equivalent meetings of the management body of the entity,

(E) authority to coordinate the management of the entity with the management of other entities towards the fulfilment of a common objective, such as, without limitation, in cases where the same natural persons are involved in the management or the management body of two or more entities,

(F) the right or ability to exercise dominant influence over another entity under a contract or in accordance with the founding act or provisions of its articles of association.

(d) Financial exposures by the credit institution to third parties secured by the provision of either collateral or personal guarantees by a member of the management body constitute contingent liabilities of that member of the management body and are therefore added to the financial exposures towards that member of the management body.

(e) When there is a financial exposure to underlying assets falling within the classes of securitisation positions or receivables in the form of Collective Investment Agencies (CISs), the credit institution shall follow the provisions of Article 390 paragraph 7 of Regulation (EU) 575/2013.

(f) The competent authority may consider that a particular person who does not fall under another provision of this Directive is nevertheless part of the related parties with a member of the management body of the credit institution. In such a case, the competent authority shall notify the credit institution in writing and shall set a time limit for compliance with the provisions of this Directive. In case of doubt as to whether two or more persons are associated, the credit institution shall submit all the details to the competent authority in writing. The competent authority shall decide on the matter and inform the credit institution in writing by setting a deadline, where applicable, in order to comply with this Directive.

(g) If the financial interests of any member of the management body are so connected with the interests of another natural or legal person or persons, or if there are close links between them or they are considered to belong to the same group of related parties, then the member of the management body and such parties shall be deemed to constitute one person, the financial exposures granted to that member of the management body or to any of them shall be added and deemed to be assigned to that member of the management body.

Role and responsibilities of the management body.

7.- (1) The duties of the management body shall be clearly defined. The responsibilities and duties of the management body shall be described in a written document and duly approved by the management body.

(2) (a) All members of the management body shall be fully aware of the structure and responsibilities of the management body, and of the division of tasks between different functions of the management body and its committees.

(b) The management body shall ensure the existence of a clear and documented division of tasks, responsibilities and powers of the management body and the committees of the management body as bodies and the members of the management body as persons, of the senior executives and of operations of the internal control system, in accordance with the provisions of the Law and of this Directive, in such a way so that:

(i) the distribution of roles, responsibilities and powers promotes the effective separation of supervisory and management functions;

(ii) it is clear who has which one of these roles, responsibilities and powers;

(iii) in the event that responsibilities have been allocated to more than one function of the credit institution, how are these responsibilities shared or distributed among the functions in question in a manner which is appropriate and clearly documented;

(iv) the business and affairs of the credit institution can be adequately monitored and controlled by the management body and by senior management;

(v) a record is kept concerning the distribution of responsibilities and powers for a term of seven (7) years from the date on which it was replaced by a more up-to-date record.

(c) In order to have appropriate checks and balances in place, the decision-making process of the credit institution shall not be dominated by a single member or by a small subset of its members.

(3) The management body's responsibilities shall include setting, approving and overseeing the implementation of the following:

(a) the overall business strategy and the key policies of the credit institution within the applicable legal and regulatory framework, taking into account the credit institution's long- term financial interests and solvency, and evaluating at least once a year the level of effectiveness of the credit institution's management of regulatory risk. The management body shall be aware of the regulatory environment in which the credit institution operates, ensure that the credit institution has an appropriate regulatory compliance framework and maintain an effective and productive relationship with the competent authorities;

(b) the overall risk strategy, including the risk appetite of the credit institution and its risk management framework and measures to ensure that the management body devotes sufficient time to risk issues;

(c) an adequate and effective internal governance and internal control framework as defined by this Directive, that includes a clear organisational structure and well-functioning independent internal risk management, compliance and audit functions as well as an ICT risk management and a security risk management function that have sufficient authority, stature and resources to perform their functions and ensures compliance with regulatory requirements related to the prevention of money laundering;

(d) the amounts, types and distribution of both internal capital and regulatory capital to adequately cover the risks of the credit institution;

(e) targets for the liquidity management of the credit institution;

EBA/GL/2015/22

(f) a remuneration policy that is in line with the remuneration principles set out in paragraphs 30 and 31 of this Directive and the EBA guidelines on sound remuneration policies;

(g) arrangements aimed at ensuring that the individual and collective suitability assessments of the management body are carried out effectively, that the composition and succession planning of the management body are appropriate, and that the management body performs its functions effectively;

(h) the selection and suitability assessment process for key function holders;

(i) arrangements aimed at ensuring the internal functioning of each committee of the management body, when established, detailing the:

(i) role, composition and tasks of each committee;

(ii) appropriate information flow, including the documentation of recommendations and conclusions, and reporting lines between each committee and the management body, competent authorities and other parties;

(j) a risk culture in line with paragraph 39 of this Directive, which addresses the credit institution's risk awareness and risk-taking behaviour;

(k) a corporate culture and values in line with paragraph 40 of this Directive, which fosters responsible and ethical conduct, including a code of conduct or similar instrument;

(l) a conflict-of-interest policy at credit institutional level in line with paragraph 41 and for staff in line with paragraph 42 of this Directive; and

(m) arrangements aimed at ensuring the integrity of the accounting and financial reporting systems, including financial and operational controls and compliance with the Law and relevant standards.

(4) When setting, approving and supervising the implementation of the aspects listed in sub-paragraph (3), the management body shall aim at ensuring a business model and governance arrangements, including a risk management framework that take into account all risks, including environmental, social and governance risks (ESG). Credit institutions shall consider that the aforementioned risks may drive their prudential risks, including credit risk, for instance through risk

factors related to the transition to a sustainable economy or with external, natural, climatic events that affect debtors, the market, liquidity, but also related to operational risks and reputational risks, for instance social factors and governance actors in the context of outsourcing. Such risks include, for instance, legal risks under contract law and labour law, risks related to possible human rights violations, or environmental, social and governance (ESG) risk factors that may affect the country where the service provider is located and its ability to provide services at agreed service levels.

(5) All members of the management body shall be informed about the overall activity, financial and risk situation of the credit institution, taking into account the economic environment, and about decisions taken that have a major impact on the credit institution's business.

(6) The management body shall ensure that the delegation of responsibilities to each member of the management body takes due account of whether each member has the competence and the level of independence and objectivity required to perform the tasks assigned to it.

(7) The management body shall check and ensure the ability of the members of the committees to allocate the necessary time for their participation in the committees. Where a member of a committee is not able to devote sufficient time to attend committee meetings, the management body shall replace such member with another member who has the necessary time, experience and competence.

(8) The management body shall monitor, review on a periodic basis and address any weaknesses identified in the implementation of the processes, strategies and policies related to the responsibilities set out in paragraphs 6 and 7 of this Directive.

(9) The management body shall periodically monitor and assess the effectiveness of the governance arrangements of the credit institution and take the appropriate actions to address any deficiencies. The Internal governance framework shall be updated in accordance with the principle of proportionality, in accordance with the provisions of paragraph 5 of this Directive. In case of any material changes affecting the credit institution, a more thorough review shall be carried out.

(10) The management body shall actively engage in the business activities of the credit institution and take decisions on a sound and well-informed basis.

(11) The management body shall be responsible for the implementation of the specified strategies and discuss regularly the implementation and appropriateness of these strategies. The operational implementation may be performed by the management of the credit institution.

(12) (a) The management body shall constructively challenge and critically review propositions, explanations and information it receives when exercising its judgment and taking decisions.

(b) The management body shall receive comprehensive reports and updates on a regular basis and where necessary without undue delay concerning relevant information for the assessment of a situation, the risks and developments affecting or that may affect the credit institution, for instance material decisions on business activities and risks taken, the evaluation of the institution's economic and business environment, liquidity and sound capital base of the credit institution, as well as the assessment of its material risk exposures.

188(I) of 2007
58(I) of 2010
80(I) of 2012
192(I) of 2012
101(I) of 2013
184(I) of 2014
18(I) of 2016
13(I) of 2018
158(I) of 2018
81(I) of 2019
13(I) of 2021
22(I) of 2021
61(I) of 2021.

(13) The management body shall appoint one of its members, in accordance with the requirements of section 58D of the Prevention and Combating of Money Laundering Law of 2007 which shall be responsible at the level of the management body for the implementation of the laws, regulations and administrative provisions required to be complied with for the purposes of compliance with the Prevention and Combatting of Money Laundering Law of 2007 and the Directives and/or circulars and/or regulations issued thereunder, including any acts of the European Union, including the relevant arrangements and procedures of the credit institution for preventing and combating money laundering. Where there is an audit committee, the person in charge shall be the chair of the audit committee.

(14) The role of members of the management body shall include monitoring and constructively challenging the credit institution's strategy.

(15) (a) The management body shall approve and periodically review the strategies and policies for taking up, managing, monitoring and mitigating the risks to which the credit institution is or could be exposed, including those posed by the macroeconomic environment in which it operates, taking into account the phase of the business cycle.

(b) The management body shall devote sufficient time to the consideration of risk issues. The management body shall be actively involved in and ensure that adequate resources are allocated to the management of all material risks addressed by this Directive, the provisions of the harmonisation with Directive 2013/36/EU and Regulation (EU) No 575/2013, as well as in the

valuation of assets, the use of external credit ratings and internal models relating to those risks. The credit institution establishes reporting lines to the management body, which cover all material risks and risk management policies as well as changes in them.

(16) (a) The management body shall ensure that the credit institution has adequate internal governance framework and internal control system for its ICT and security risks. The management body shall set clear roles and responsibilities for the section or sections responsible for ICT systems, information security risk management and business continuity, including those of the management body itself and its committees.

(b) The management body shall ensure that the quantity and skills of the staff members of the credit institution are adequate to support its ICT operational needs and ICT and security risk management processes on an ongoing basis, as well as to ensure the implementation of the relevant ICT strategy. The management body shall ensure that the allocated budget is appropriate for the fulfilment of the above obligations.

(c) The management body shall have overall accountability for setting, approving and overseeing the implementation of the ICT strategy of the credit institution in the context of its overall business strategy, as well as for the establishment of an effective risk management framework for the ICT and security risks.

Cap. 113
9 of 1968
76 of 1977
17 of 1979
105 of 1985
198 of 1986
19 of 1990
46(I) του1992
96(I) of 1992
41(I) of 1994
15(I) of 1995
21(I) of 1997
Announcement
2331
82(I) of 1999
149(I) of 1999
2(I) of 2000
135(I) of 2000
151(I) of 2000
76(I) of 2001
70(I) of 2003
167(I) of 2003
92(I) of 2004
24(I) of 2005
129(I) of 2005
130(I) of 2005
98(I) of 2006
124(I) of 2006
70(I) of 2007
71(I) of 2007
131(I) of 2007
186(I) of 2007
87(I) of 2008
41(I) of 2009
49(I) of 2009
99(I) of 2009
42(I) of 2010
60(I) of 2010
88(I) of 2010
53(I) of 2011
117(I) of 2011
145(I) of 2011
157(I) of 2011
198(I) of 2011
64(I) of 2012
98(I) of 2012
190(I) of 2012
203(I) of 2012
6(I) of 2013

(17) Without prejudice to its duties under the Companies Law, the management body shall perform the following supervisory duties:

90(I) of 2013
74(I) of 2014
75(I) of 2014
18(I) of 2015
62(I) of 2015
63(I) of 2015
89(I) of 2015
120(I) of 2015
40(I) of 2016
90(I) of 2016
97(I) of 2016
17(I) of 2017
33(I) of 2017
51(I) of 2017
37(I) of 2018
83(I) of 2018
149(I) of 2018
163(I) of 2019
38(I) of 2020
43(I) of 2020
191(I) of 2020
192(I) of 2020
32(I) of 2021
43(I) of 2021.

(a) oversee and monitor management decision-making and actions and provide effective oversight of the management body, including monitoring and scrutinising its individual and collective performance and the implementation of the credit institution's strategy and objectives;

(b) constructively challenge and critically review proposals and information provided by the senior management , as well as their decisions, as well as their performance in fulfilling the agreed goals and objectives;

(c) taking into account the proportionality principle as set out in Part II, appropriately fulfil the duties and role of the risk committee, the remuneration committee and the nomination committee, where no such committees have been set up;

(d) ensure and periodically assess the effectiveness of the credit institution's internal governance framework and take appropriate steps to address any identified deficiencies;

(e) oversee and monitor that the credit institution's strategic objectives, organisational structure and risk strategy, including its risk appetite and risk management framework, as well as other policies, for instance the remuneration policy, and the disclosure framework are implemented consistently;

(f) monitor that the risk culture of the credit institution is implemented consistently;

(g) oversee the implementation and maintenance of a code of conduct or similar and effective policies to identify, manage and mitigate actual and potential conflicts of interest;

(h) oversee the integrity of financial information and reporting, and the internal control framework, including an effective and sound risk management framework;

(i) ensure that the heads of internal control functions are able to act independently and, regardless the responsibility to report to other internal bodies, business lines or units, can raise concerns and warn the management body in its supervisory function directly, where necessary, when adverse risk developments affect or may affect the credit institution;

(j) monitor the implementation of the internal audit plan, after the prior involvement of the risk and audit committees;

(k) has a central role in the appointment, and where necessary, in the removal of senior management, and in the planning of the succession of such staff and

(l) provide objective views on resources, appointments and standards of conduct.

(18) The management body shall establish appropriate procedures for assessing whether the credit institution operates within its approved strategies and in this regard the management body shall set clear and objective performance targets for senior management concerning both the credit institution and senior executives.

(19) The independent members of the management body maintain, in any case, independence of thought and opinion.

(20) The members of the management body shall be responsible for their role and duties as prescribed by applicable law and by the instructions of the competent authority. Each member of the

management body shall not cease to be liable for his role and responsibilities for the duration of his appointment as a member of the management body.

Size and composition of the management body.

8.- (1) The size and composition of the management body shall be determined taking into account the principle of proportionality, ensuring that the majority of the members and the chair of the management body are independent, as set out in paragraph (1) of section 19B of the Law. In particular, the following shall be ensured–

(a) the management body shall consist of at least seven (7) members and not more than thirteen (13) members;

(b) the executive members shall be at least two (2) and not more than twenty five percent (25%) of the members of the management body rounded down, one of whom is the managing director;

(2) The members of the management body may not appoint alternate members to represent them in case of their absence.

(3) The head of the internal control system may not be appointed as member of the management body.

(4) In relation to the organisational structure of the management body:

(a) the position of chairman of the management body, in accordance with the provisions of section 19B of the Law, shall be held by an independent member of the management body;

(b) the position of Vice-Chairman of the management body shall be held by a non-executive member, and assume the roles and responsibilities of the chairman in the absence of the latter;

(c) an independent member of the management body shall be appointed as a senior independent member;

Provided that the senior independent member of the management body cannot hold the position of chairman or vice-chairman;

(d) committees of appropriate size, composition, structure and responsibilities shall be established for the effective performance of the roles and responsibilities of the management body, in accordance with the provisions of Section II of this Part.

Role of the chair of the management body.

9.- (1) The chair of the management body shall lead the management body, contribute to an efficient flow of information, both within the management body and between the management body and its committees, and shall also be responsible for the effective overall functioning of the management body.

(2) The chair of the management body shall encourage and promote an open and critical discussion and ensure that dissenting views can be expressed and discussed within the decision-making process.

(3) The chair of the management body shall set the items on the agenda of the meetings and ensure that strategic issues are discussed as a matter of priority.

(4) (a) The chair of the management body shall ensure that the decisions of the management body are taken on a sound basis and after adequate information and ensure that the relevant documents and information are received in a timely manner before the meeting.

(b) The chair of the management body shall ensure that the members of the management body are given sufficient time to consider important issues and receive answers to any questions or concerns they may have, without being faced with unrealistic deadlines for taking decisions.

(5) The chair of the management body shall contribute to the clear allocation of duties between the members of the management body and ensure the existence of an efficient flow of information between them, so as to enable members to constructively contribute to the discussions and to cast their votes on a sound and well informed basis.

(6) The chair of the management body shall be responsible for ensuring compliance with paragraphs 11 and 12 of this Directive, through appropriate procedures and actions.

(7) Subject to the requirements of paragraph 42 of this Directive, the chair of the management body shall ensure, through an explicit procedure, the notification of conflicting interests to the management body and the abstention of members from the process of discussion, decision-making or voting on any issue for which they may have a conflict of interest.

(8) The chair of the management body shall maintain adequate contact with the competent authority and other supervisory authorities and ensure that the views and concerns of the supervisory authorities and any views and concerns of shareholders that he becomes aware of, are communicated in their entirety to the management body.

(9) The chair of the management body:

(a) shall be in charge of ensuring that the procedures are followed (for instance within the framework of proper functioning of the nomination committee) so that the members of the management body have at all times sufficient knowledge and the skills to perform their duties; the chair shall ensure compliance with the procedures for the participation of new members of the management body in an introductory training program, in accordance with paragraphs 16 and 17 of the Assessment of the Directive on the Assessment of Suitability of the Members of the Management Body and Key Function Holders of Authorised Credit institutions of 2020;

(b) shall be in charge of ensuring compliance with the procedures for the recognition of the training needs of the members of the management body on an individual basis as well as of the management body as a whole, based on the reports submitted at least annually by the nomination committee in accordance with paragraph 23 (1) of this Directive, and to ensure that these needs are met;

(c) shall be in charge of ensuring that the Evaluation of the management body, its committees and each member of the management body is carried out in accordance with the provisions of paragraph 16 and that the credit institution takes action commensurate with the results of those assessments; recognising the strengths and addressing the weaknesses of the management body.

Senior independent member of the management body.

10.- The duties of the senior independent member of the management body, appointed in accordance with point (c) of sub-paragraph (4) of paragraph 8 of this Directive, shall include, inter alia, the following:

(a) to act as a point of contact with shareholders and other stakeholders regarding concerns that could not be addressed or resolved or that could not be addressed or resolved through the usual channels of communication with the chairman of the management body or senior management;

(b) to ensure that the management body has a balanced understanding of the most significant issues and concerns of shareholders;

(c) to chair the meetings with the non-executive members of the management body, without the presence of the chairman, at least annually, in order to evaluate the performance of the chairman in accordance with paragraph 11 of this Directive;

(d) to chair the management body during the examination of the succession of the chairman of the management body and to ensure the smooth process of succession.

Meetings of the management body.

11.- (1) With regards to the organisation of the meetings of the management body and its committees:

(a) the management body and its committees hold ordinary meetings for the adequate and efficient performance of their duties;

(b) every effort is exercised to hold at least once a year a management body's regular meeting with the physical presence of all members;

(c) the non-executive members of the management body hold regular meetings on their own or with the external auditors and/or the heads of the internal control functions as appropriate, without the presence of the executive members, at least on a semi-annual basis;

(d) the non-executive members of the management body meet in the absence of the chairman at least annually to appraise the chairman's performance;

(e) the arrangement of attending scheduled or special meetings via teleconferencing or videoconferencing shall not be abused but used with caution at the member, and management body level ensuring that, as a rule and where there are no special circumstances to justify the opposite, at least the majority of the members are physically present at any ordinary or ad hoc meeting;

(f) the members of the management body may not be absent from ordinary or ad hoc meetings, whether physically or via teleconferencing, for more than two (2) consecutive meetings or twenty five percent (25%) of the annual meetings;

(g) proxy voting may be permitted for to a member who is absent from a meeting, if the exercise of proxy voting is limited to one (1) per annum per each member attending the meeting and members who vote via proxy are held accountable for their proxy vote;

(h) persons nominated by the credit institution for the position of member of the management body for which the decision of the competent authority is pending are prohibited to be present as observers.

Provided that the person performing the duties of temporary deputy managing director, may attend the meetings of the management body, only upon relevant invitation of the management body, for specific issues and for specific reasons related to his executive duties. Subject to the requirements

of section 18 of the Law, this person is not present at the part of the meetings concerning the discussions and decision-making of the management body.

(2) With regards to the treatment of interest or conflict of interest or potential interest or conflict of interest of members of the management body:

(a) a review or approval process is in place which the members of the management body shall follow before they engage in certain activities such as serving on another entity's management body, to ensure such new engagement would not create a conflict of interest;

(b) a requirement that members shall disclose any conflicts of interests and abstain from participating in the decision-making or voting on any matter where they may have a conflict of interest; in particular:

(i) prior to the commencement of any meeting the acting chairman of the meeting is required to read all items on the agenda, one by one, and request that each participant, including himself and the members, for each item states clearly whether there is an interest or a conflict of interest or a potential interest or conflict of interest or not;

Provided that, a proxy holder shall in addition state for each item whether the member he represents has an interest or a conflict of interest or a potential interest or conflict of interest or not;

(ii) upon completion of the procedure referred to in subpoint (i), the chair shall invite comments from all members participating in the meeting regarding the statements made;

(iii) if a conflict of interest is identified for an item of the agenda, then the member involved shall abstain from the discussion and from the voting for that particular item either in person or via proxy;

(iv) if any other/ ad hoc issues are discussed, then an analogous process shall be followed;

(c) the manner in which the management body would deal with any non-compliance with the policies, practices and procedures on conflicts of interest; such non-compliance shall be communicated immediately to the Central Bank.

Minutes of the meetings of the management body.

12.- With regards to the documentation of minutes of meetings of the management body and its committees:

(a) detailed minutes shall be kept for each meeting which shall be finalised not later than fifteen (15) business days following the meeting and formally approved at the next meeting;

(b) the minutes of the meeting shall record –

(i) the time of meeting, location held and attendees including invitees, physically and via electronic media;

(ii) the reasoning for inviting persons to attend the meeting in accordance with point (h) of paragraph 11, the relevant item(s) on the agenda and their views and/or opinions;

(iii) all items on the agenda and the respective discussions, decisions, voting results, opinions and views of the minority, as well as concerns not resolved;

(iv) the statements referred to in point (b) of subparagraph (3) recorded separately under the title 'identification of interests or conflicts of interest or potential interests or conflicts of interest".

Role and responsibilities of the secretary.

13.- (1) Credit institutions shall appoint a person who will perform the duties of the secretary under section 171 of the Companies Law.

(2) Having regard to the provisions of sections 172 and 173 of the Companies Law, credit institutions shall take care to avoid any conflict of interest in appointing the secretary.

The secretary may delegate tasks referred to in this paragraph to third persons provided there is no conflict of interest and the secretary checks and signs paperwork and remains responsible and accountable for the outcomes of the delegation.

Provided that the secretary may not delegate his tasks to the heads of the internal control functions.

(3) The secretary shall ensure that the management body and its committees are constituted and function in compliance with internal rules and regulations of the management body, the provisions of this Directive and other applicable legal and supervisory requirements.

(4) The secretary shall act as a source of information and advice to members of the management body, ensure adequate information flows within the management body and its committees, between senior management and non-executive members and between heads of internal control functions and non-executive members.

(5) (a) The secretary shall arrange induction programmes for non-executive members of the management body which provide a full, formal and tailored introduction to the credit institution and to their duties and responsibilities.

(b) The secretary shall assist the chair of the management body in assessing and meeting the training needs of members of the management body and ensure that there is an ongoing programme to keep members well informed of developments in the company and in respect of matters relevant to their responsibilities generally.

(6) The secretary shall ensure that non-executive members have access to independent professional advice at the credit institution's expenses if required.

(7) The secretary shall be closely involved in preparing the schedule of all management body and committee meetings and shall have an obligation to:

(a) prepare the agendas for these meetings in cooperation with the chairman, ensuring matters which require the attention or action of the management body, or a committee are included in the items of the agendas;

(b) ensure that relevant information is dispatched timely to all members of the management body to enable them to prepare adequately for these meetings.

(8) The secretary shall ensure minutes are kept in accordance with paragraph 12 of this Directive and shall have an obligation to –

(a) explicitly express, in a separate paragraph, his assessment as to whether the meeting had been held in compliance with internal rules and regulations of the management body, the provisions of this Directive and other applicable legal and supervisory requirements;

(b) ensure minutes are circulated, finalised and approved in a timely manner by all members present at the meeting;

(c) ensure finalised minutes are distributed in a timely manner to all recipients;

(d) ensure decisions taken are properly communicated, pursue follow up actions and report on matters arising.

(9) The secretary shall provide support to the management body, to the chair of the management body and/or to the nomination committee in setting succession planning and overseeing succession and rotation of tasks of non-executive members of the management body.

Access of the management body and of the committees to sources and information.

14.- (1) (a) The management body in the exercise of its supervisory function, and all its committees, shall have adequate access to information concerning their duties.

(b) The management body shall determine the framework and appropriate and transparent procedures for this access, and appropriate and transparent procedures in case it allows its members to communicate individually and directly with the senior management and/or members of staff of the credit institution, in the exercise of their supervisory responsibilities as members of the management body or and its committees.

(c) The management body and the risks committee, where a risk committee has been established according to the provisions of section II of this Part, shall have adequate access to information on the risk situation of the credit institution and, if necessary and appropriate, to the risk management function and to external expert advice.

(2) The management body and the risks committee, which is established according to the provisions section II of this Part, shall determine the nature, the amount, the format, and the frequency of the information on risk which it is to receive.

Nomination, selection, and succession of members of the management body.

15.- (1) Credit institutions and the respective nomination committees shall engage a broad set of qualities and competences when recruiting members and re-appointing existing members to the management body and for that purpose they shall put in place a policy promoting diversity on the management body.

(2) Credit institutions shall have in place an appropriate recruitment policy for the nomination, selection, reappointment and succession of the members of the management body which shall include, as a minimum, the following:

(a) a description of the necessary competences, skills and academic or professional qualifications to ensure sufficient expertise and conformity with the requirements of this Directive and the provisions of the Assessment of Suitability of the Members of the Management Body and Key Function Holders of Authorised Credit institutions of 2020;

(b) a requirement that, prior to appointment of new members, candidates satisfy themselves that they have the knowledge, skills, experience and time to make a positive contribution to the management body;

(c) a requirement that, the nomination committee prepares for the management body a description of how it ended up with its recommendation of candidates to fill in management body vacancies in the management body;

(d) a requirement to provide sufficient information to shareholders for the election of an individual as a member of the management body, including:

(i) a description of the individual's qualifications, experiences and competences;

(ii) a description of the roles and responsibilities for that particular vacancy;

(iii) the time commitment expected;

(iv) an explanation of the reasons it considers the appointment of that individual to be appropriate;

(e) a requirement that re-appointment is based on the performance of the member as evidenced in the appraisal reports;

(f) an appropriate succession plan for its members that considers, inter alia, the expiry date of each member's contract or mandate to prevent too many members of the management body having to be replaced simultaneously.

(3) Credit institutions shall define the maximum number of terms an individual may serve as a non-executive member of the management body subject to the provisions the Assessment of Suitability of the Members of the Management Body and Key Function Holders of Authorised Credit institutions of 2020.

(4) Credit institutions shall define the maximum number of terms an individual may serve as a chair of the management body or a management body committee; in any case an individual may serve in the position of the chair of the management body or chair of the committee of the management body for a maximum of six (6) years whether consecutive or not.

(5) The appointed members of the management body are subject to re-election at the Annual General Meeting, every 3 years from the date of their appointment.

(6) Credit institutions shall devote adequate human and financial resources to the induction and training of members of the management body.

Evaluation of the management body.

16.- (1) Credit institutions shall have in place an appropriate methodology and process for the in-depth and rule-based evaluation of the performance of the management body at least on an annual basis. The evaluation process shall cover, at least, the following:

(a) the performance of the management body as a whole, of committees and of individual members;

(b) the contribution of the management body as a whole, of committees and of individual members to–

(i) the development the business objectives, risk appetite and strategies;

(ii) setting and overseeing the risk and compliance management frameworks;

(iii) establishing and maintaining consistent organisational and operational arrangements and internal control mechanisms;

(c) the composition of the management body and its committees;

(d) the communication with management, shareholders and competent authority;

(e) the roles of chairperson of the management body, company secretary and senior independent member of the management body;

(f) the time commitment of non-executive members and capacity to critically review information;

(g) evaluation of the fitness and probity of each member of the management body based on the applicable criteria of the Directive on the Assessment of Suitability of the Members of the Management Body and Key Function Holders of Authorised Credit Institutions of 2020;

It is provided that, if at any given time, persons who possess the post of an independent member do not satisfy or seem not to satisfy any of the independence criteria due to some developments, then the management body shall address the issue immediately in accordance with paragraphs 25 and 27 of the Directive on the Assessment of Suitability of the Members of the Management Body and Key Function Holders of Authorised Credit Institutions of 2020, and proceed with the necessary remedial measures, including removing the said member from the management body or re-

determining his or her role in the management body and/or appointing a new independent member; the time period for implementing all necessary remedial measures shall not exceed one (1) month.

It is further provided that the said member shall be released from any duties which were carried out by him or her as an independent member of the management body from the date the non-compliance with the independence criteria is identified.

(2) Credit institutions shall assign at least every three (3) years the review and evaluation of the composition, efficiency and effectiveness of the management body and its committees to an independent external consultant having regard to the requirements of this Directive and to bring an objective perspective and share leading industry practices.

Section II – Committees of the management body

Setting up committees of the management body.

17.- (1) Credit institutions shall establish a risk, a nomination and a remuneration committee to advise the management body and to prepare the decisions to be taken by this body.

Provided that credit institutions shall also establish an audit committee in accordance with the provisions of section 78 of the Auditors Law.

53(I) of 2017
171(I) of 2017
7(I) of 2018.

(2) The competent authority may authorise a credit institution that is not considered significant in terms of size, internal organisation and nature, scope and complexity of its activities, not to establish one or more of these committees, at the request of the credit institution, provided that:

(a) in case the credit institution is a subsidiary of a group, the relevant duties are exercised by the respective committees of the parent company which submit their recommendations and decisions to the management body of the credit institution; or

(b) the relevant duties are performed by the Combined Committees according to the provisions of paragraph 24 of this Directive.

(3) In the event that the competent authority has authorised a credit institution not to set up one or more of the risk, nomination or remuneration committees under sub-paragraph (2) of paragraph 17 of this Directive, references to those committees in this Directive shall be construed as applying to the management body of the credit institution or to its Combined Committees, respectively.

(4) Credit institutions may establish other committees, for instance, ethics, conduct and compliance committees and/or committee on preventing and combating money laundering, taking into account the criteria specified in Part 2 of this Directive.

(5) Credit institutions shall ensure a clear allocation and distribution of duties and tasks between specialised committees of the management body.

(6) Each committee shall have a documented mandate, including the scope of its responsibilities, from the management body in its supervisory function and establish appropriate working procedures.

(7) Committees shall support the supervisory function in specific areas and facilitate the development and implementation of a sound internal governance framework. Delegating to committees does not in any way release the management body from collectively fulfilling its duties and responsibilities.

Composition of committees of the management body.

18.- (1) The independent members of the management body shall be actively involved in the committees. For the mandatory committees referred to in paragraph 17 of this Directive, more than fifty percent (50%), of the committee members shall be independent members.

(2) The committees of the management body shall be composed of at least three members.

(3) Considering the size of the management body and the number of independent members of the management body, credit institutions shall ensure that participation in more than one committee ensures that no individual exerts too much influence or control over them. In any event, a member of the management body may not be a member in more than two (2) committees referred to in paragraph 17 (1) of this Directive.

(4) Credit institutions shall consider the occasional rotation of chairs and members of committees, taking into account the specific experience, knowledge and skills that are individually or collectively required for those committees.

(5) All committees of the management body shall be composed of non-executive members of the management body.

(6) Subject to the requirements of section 78 of the Auditors Law regarding the composition of the audit committee, the chair of the management body may not be a member of the audit committee.

(7) (a) With regard to the requirements of sub-paragraph (1) in relation to the remuneration committee, if there is no sufficient number of qualified independent members, credit institutions shall

apply other measures within the scope of the remuneration policy in order to reduce conflicts of interest in decision-making on remuneration issues.

(b) The members of the remuneration committee shall have, collectively, appropriate knowledge, expertise and professional experience in remuneration policies and practices, risk management and control activities, in particular as regards to the mechanism for aligning the remuneration structure with the risk and capital profile of the credit institution.

(8) (a) The nomination committee shall be chaired by an independent member in case the credit institution is a systemically significant credit institution (G-SII) or another systemically significant credit institution (O-SII). In accordance with the principle of proportionality, other credit institutions may also consider as a good practice having a chair of the nomination committee who is independent.

(b) The members of the nomination committee shall have individually and collectively appropriate knowledge, skills and expertise regarding the candidate selection process and their suitability requirements.

(9) (a) The risk committee shall be chaired by an independent member in case the credit institution is a systemically significant credit institution (G-SII) or another systemically significant credit institution (O-SII). For other credit institutions, the risk committee shall, where possible, be chaired by an independent member. In all credit institutions, the chair of the risk committee shall neither be the chair of the management body nor the chair of any other committee.

(b) The members of the risk committee shall have, individually and collectively, the appropriate knowledge, skills and expertise to fully understand and monitor the risk strategy and risk-taking policy of the credit institution, as well as its management and risk control practices.

(10) The members of a committee must not hold any other positions or carry on any transactions that could be considered to be in conflict with the terms of the committee.

Committee proceedings.

19.-(1) Committees shall submit reports on an ordinary basis and communicate their minutes to the management body before the meetings of the management body.

(2) Committees shall interact with each other appropriately. Subject to sub-paragraph (4) of paragraph 18 of this Directive, such interaction could take the form of cross-participation so that the chair or a member of one committee could also be a member of another committee.

(3) The members of committees shall engage in open and critical discussion in the meetings of the committees during which divergent views are discussed in a constructive manner.

(4) Committees shall document the agenda of their meetings, as well as their main results and conclusions.

(5) The risk and nomination committees shall at least:

(a) have access to all relevant information and data necessary to perform their role, including information and data from relevant corporate and audit functions, for instance legal, financial, human resources, technology and IT section, audit, risk, ICT and security function, regulatory compliance, including information on regulatory compliance, in order to prevent and combat money laundering, including access to aggregate information and risk factors related to preventing and combating money laundering;

(b) receive regular reports, ad hoc information, communications and opinions from the heads of the internal control functions regarding the current risk profile of the credit institution, its risk management culture and risk limits, as well as any material breaches that may have arisen, with detailed information on and recommendations for corrective measures taken, to be taken or suggested in order to address them;

(c) periodically review and decide on the content, format and frequency of the information to be reported to them regarding the risk; and

(d) where necessary, to ensure the proper involvement of the internal control functions and other relevant functions (human resources, legal, finance) within their respective areas of expertise and/or to seek advice from external experts.

(6) Subject to the provisions of paragraphs 20, 21, 22 and 23 of this Directive, the duties, tasks and responsibilities of the risk, audit, remuneration and nomination committees may not be delegated to another committee, unless a combined committee according to the provisions of paragraph 24 of this Directive is established.

(7) (a) The provisions of paragraph 9 of this Directive shall apply mutatis mutandis to the chairmen of each committee of the management body.

(b) The provisions of paragraphs 11 and 12 of this Directive shall apply mutatis mutandis to the committees of the management body.

(8) (a) All committees of the management body shall perform an annual self-assessment and submit reports to the management body with conclusions and suggestions for improvements and changes.

(b) Subject to sub-paragraph (8) of paragraph 7 of this Directive, all committees shall annually review their terms of reference and submit reports to the management body with conclusions and suggestions for improvement.

(9) The chair of each committee shall ensure that no person other than the members of the committee is present at a meeting of the committee, including other members of the management body, unless formally invited to attend for a specific item on the agenda; any such person shall be present only for the presentation of the specific issue and shall leave the conference room immediately afterwards, without any participation in the decision-making process.

Role of the risk committee.

20.- (1) The risk committee shall at least:

(a) advise and support the management body regarding the monitoring of the credit institution's overall actual and future risk appetite and strategy, taking into account all types of risks, to ensure that they are in line with the business strategy, objectives, corporate culture and values of the credit institution;

(b) assist the management body in overseeing the implementation of the credit institution's risk strategy and the corresponding limits set; the management body shall bear full responsibility for the proper and adequate management of the risks;

(c) oversee the implementation of the strategies for capital and liquidity management as well as for all other relevant risks of a credit institution, such as market, credit, operational (including legal and IT risks) and reputational risks, and, based on the work of the audit committee, the risk management function and the external auditors, in order to assess their adequacy against the approved risk appetite and strategy and to evaluate the adequacy of the forecasts and the effectiveness of the strategies and policies regarding maintenance, in continuous basis, sufficient amounts, types and distribution of internal capital and equity to cover the risks of the credit institution;

(d) provide the management body with recommendations on necessary adjustments to the risk strategy resulting from, inter alia, changes in the business model of the credit institution, market developments or recommendations made by the risk management function;

(e) provide advice on the appointment of external consultants that the supervisory function may decide to engage for advice or support;

(f) review a number of possible scenarios, including stressed scenarios, to assess how the credit institution's risk profile would react to external and internal events;

(g) oversee the alignment between all material financial products and services offered to clients and the business model and risk strategy of the credit institution by taking into account the EBA guidelines on product oversight and governance arrangements for retail banking products. The risk committee shall assess the risks associated with the offered financial products and services and take into account the alignment between the prices assigned to and the profits gained from those products and services. The risk committee shall review whether the prices of liabilities and assets offered to clients fully take into account the business model and the risk strategy of the credit institution. Where the prices do not properly reflect the risks in accordance with the business model and the risk strategy, the risk committee shall present a remedy plan to the management body;

(h) assess the recommendations of internal or external auditors and follow up on the appropriate implementation of measures taken.

(2) The risk committee shall collaborate with other committees of the management body whose activities may have an impact on the risk strategy (for instance, audit and remuneration committees) and regularly communicate with the credit institution's internal control functions, in particular the risk management function and the ICT and Security function.

(3) The risk committee shall submit to the management body suggestions for the appointment or removal of the head of the risk management function and of the ICT and security risk management function.

(4) The risk committee shall perform an annual assessment of the head of the risk management function and of the ICT and security function and submit it to the management body.

(5) The risk committee shall evaluate and monitor the independence, adequacy and effectiveness of the risk management function and the ICT and security function, and shall advise the management body thereon, as well as on the adequacy and effectiveness of the information security framework,

which shall inter alia ensure the adequate protection of the confidential and proprietary information of the credit institution.

(6) The risk committee shall review and approves the budgets of the risk management function and of the ICT and security risk management function, ensuring that they are flexible enough to adapt to changes depending on developments.

(7) the risk committee shall, without prejudice to the tasks of the remuneration committee, and in order to contribute to the formation of sound political and practical remuneration, examine whether incentives provided by the system, policies and practices take into consideration the credit institution's risk, capital and liquidity and the likelihood and timing of earnings.

Role of the audit committee.

21.- (1) Subject to the provisions of the Auditors Law, the audit committee shall, inter alia:

(a) monitor the effectiveness of the credit institution's internal quality control and risk management systems and, where applicable, its internal audit function, with regard to the financial reporting of the audited credit institution, without breaching its independence;

(b) evaluate and monitor the independence and adequacy of the internal audit function;

(c) oversee the establishment of accounting policies by the credit institution;

(d) monitor the financial reporting process and submit recommendations aimed at ensuring its integrity;

(e) review and monitor the independence of the statutory auditors or the audit firms in accordance with sections 58, 59, 60, 63 and 64 of the Auditors Law and Article 6 of Regulation (EU) No 537/2014, and in particular the appropriateness of the provision of non-audit services to the audited credit institution in accordance with Article 5 of Regulation (EU) No 537/2014;

(f) monitor the statutory audit of the annual and consolidated financial statements, in particular its performance, taking into account any findings and conclusions by the competent authority pursuant to Article 26(6) of Regulation (EU) No 537/2014;

(g) be responsible for the procedure for the selection of external statutory auditor(s) or audit firm(s) and recommend for approval by the credit institution's competent body their appointment, in accordance with Article 16 of Regulation (EU) No 537/2014, compensation and dismissal;

(h) review the audit scope and frequency of the statutory audit of annual or consolidated accounts;

(i) inform the administrative or supervisory body of the audited entity in accordance with paragraph (a) of subsection 5 of Article 78 of the Auditors Law of the outcome of the statutory audit and explain how the statutory audit contributed to the integrity of financial reporting and what the role of the audit committee was in that process; and

(j) receive and take into account audit reports.

(2) The audit committee shall assist the management body in overseeing the independence, adequacy and effectiveness of the compliance function, or in case the compliance function is performed in conjunction with another audit function in accordance with paragraph 55 of this Directive, the audit committee shall evaluate and monitor the independence, adequacy and effectiveness of the compliance function within the combined audit function. In particular, the audit committee shall ensure of the following:

(a) advising the management body, based on the work of the compliance function, on the adequacy and effectiveness of the business ethics framework;

(b) advising the management body, based on the work of the compliance function and the external auditors, on the adequacy and effectiveness of the compliance framework;

(3) The audit committee shall ensure the examination and provide assistance to the management body regarding the approval of the annual control program of the internal audit function and the regulatory compliance program of the compliance function;

(4) The audit committee shall submit recommendations to the management body for the appointment or removal of the heads of internal audit and compliance functions;

(5) The audit committee shall carry out an annual assessment of the heads of the internal audit and compliance functions and shall then submit them to the management body;

(6) The audit committee shall assist the management body in reviewing and approving the budgets of the internal audit and compliance functions, ensuring that they are flexible enough to adapt to changes according to developments;

(7) The audit committee shall oversee the timely adoption of necessary corrective action by senior management to address audit deficiencies, non-compliance with the credit institution's policies, laws

and regulations, and other weaknesses identified by external auditors. internal audit and compliance functions and by supervisory authorities;

(8) The audit committee shall assist the management body in reviewing, monitoring and approving the official announcements of the credit institution regarding the financial performance and other disclosures.

Role of the remuneration committee.

22.- (1) The remuneration committee shall be constituted in such a way as to enable it to exercise competent and independent judgment on remuneration policies and practices and the incentives created for managing risk, capital and liquidity. It shall support and advise the management body regarding the planning and/or updating and monitoring of the implementation of the remuneration policy and practices and compliance with them.

(2) The remuneration committee shall be responsible for the preparation of decisions regarding remuneration, including those which have implications for the risk and risk management of the credit institution and which are to be taken by the management body.

(3) When preparing the decisions referred to in sub-paragraph (2), the remuneration committee shall take into account the long-term interests of shareholders, investors and other stakeholders of the credit institution and the public interest and ensure that:

(a) these are closely related to the business objectives and strategies of the credit institution;

(b) these are in accordance with the requirements specified in Part 4 of this Directive;

(c) non-executive members are not among the beneficiaries of performance-related remuneration.

(4) The remuneration committee shall ensure that internal control functions are involved in the design, review and implementation of the remuneration policy.

(5) The remuneration committee shall ensure that members of staff involved in the design, review and implementation of remuneration policies and practices have relevant experience and are able to form an independent opinion on the appropriateness of remuneration policies and practices, including their suitability for risk management.

Role of the nomination committee.

23.- (1) The main duties and responsibilities of the nomination committee shall include the following:

(a) identifying and recommending, for the approval of the management body or for approval of the general meeting, candidates to fill management body vacancies, evaluating the balance of knowledge, skills, diversity and experience of the management body and preparing a description of the roles and capabilities for a particular appointment, and assessing the time commitment expected for that position;

(b) assessing periodically, and at least annually the structure, size, composition and performance of the management body and making recommendations to the management body with regard to any changes;

(c) assessing periodically, and at least annually, the knowledge, skills and experience of individual members of the management body and of the management body collectively, and reporting to the management body accordingly;

(d) reviewing periodically, and at least annually, succession plans for the management body to ensure on the one hand that successions occur smoothly and an appropriate balance of diversity, skills and experience is maintained and on the other hand the progressive renewal of the management body, and reporting to the management body accordingly;

(e) reviewing periodically, and at least annually, the policy of the management body for selection, development, appointment and replacement of senior management and heads of internal control functions and making recommendations to the management body.

(f) reviewing periodically the policy of the credit institution for recruitment, rotation and promotion of staff and reporting to the management body accordingly;

(g) reviewing periodically, and at least annually, in collaboration with the audit and risk committee, the composition, authority and independence of internal control functions and reporting to the management body accordingly;

(2) For the purposes of subparagraph (1)(a), the nomination committee shall decide on a target for the representation of the underrepresented gender in the management body and prepare a policy on how to increase the number of the underrepresented gender in the management body in order to meet that target; the target, policy and its implementation shall be made public in accordance with Article 435(2)(c) of Regulation (EU) No 575/2013.

(3) In performing its duties, the nomination committee shall, to the extent possible and on an ongoing basis, take account of the need to ensure that the management body's decision making is not

dominated by any one individual or small group of individuals in a manner that is detrimental to the interests of the credit institution as a whole.

(4) The nomination committee shall be able to use any forms of resources that it considers to be appropriate, including external advice, and shall receive appropriate funding to that effect.

Combined Committees.

24.- (1) H competent authority may allow credit institutions that are not considered significant in terms of size, internal organisation and nature, scope and complexity of its activities to establish:

(a) a combined committee consisting of the risk committee and the audit committee and/or

(b) a combined committee consisting of the nomination committee and the remuneration committee.

(2) Credit institutions intending to set up a combined committee shall apply to the competent authority and document the reasons why they have chosen to set up a combined committee, as well as how this approach achieves the objectives of the committees.

(3) In any event, credit institutions shall ensure that the members of a combined committee as referred to in sub-paragraph (1) have, individually and collectively, the knowledge, skills and expertise required to fully understand the tasks shall be performed by a combined committee.

PART 4 - SENIOR MANAGEMENT

Sufficient number and know-how of senior management.

25.- (1) Senior management shall be of sufficient size and have the necessary expertise to effectively direct the operations of the credit institution.

(2) Credit institutions shall ensure that senior managers assume the roles of the heads of internal control functions in accordance with the provisions of this Directive and that these individuals have no direct responsibilities over business and support units which the internal control functions under their responsibility monitor and control.

Selection, development and succession of senior management.

26.- (1) Credit institutions shall have appropriate policies and procedures in place for selecting, developing and, when appropriate, replacing the chief executive officer or other senior managers and appropriate succession plans, having due regard to the importance and critical nature of their duties vis-à-vis the operations and internal control functions of the credit institution and its group; these policies, plans and procedures shall ensure:

(a) the identification and regular updating of the necessary competencies, skills and academic or professional qualifications to ensure –

(i) the effectiveness of chief executive officer and other senior managers and heads of internal control functions in carrying out their duties and responsibilities;

(ii) conformity with regulatory requirements;

(b) that the monitoring of the development and progression of potential internal candidates is monitored and periodically reviewed against the required competencies, skills and qualifications;

(c) that the succession planning for chief executive officer and other senior managers considers the expiry date of each individual's term, mandate or contract –

(i) to prevent too many senior managers having to be replaced simultaneously;

(ii) to ensure that these transitions occur smoothly with minimum disruption to the operations of the credit institution;

(d) that emergency succession plans are in place for contingencies such as departure, death or disability of the chief executive or other senior managers to facilitate the transition to both interim and longer-term leadership in the event of an untimely vacancy.

Roles and responsibilities of the senior management

27.- (1) The chief executive officer and other senior managers are responsible for directing and overseeing the effective management of the credit institution within the authority delegated to them by the management body and in compliance with applicable laws and regulations.

(2) Senior management is responsible for:

(a) managing and overseeing the day-to-day operations of the credit institution, subject to the business objectives, strategies and policies approved by the management body as well as to legal and regulatory requirements;

(b) providing the management body with recommendations, for its review and approval, on business objectives, strategies, business plans and major policies that govern the operation of the management body;

(c) providing the management body with comprehensive, relevant and timely information that will enable it to review business objectives, business strategy and policies, and to hold senior management accountable for its performance.

Overseeing the operations of the credit institution and providing direction on a day-to- day basis.

28.- (1) Senior management is responsible for implementing an effective and transparent operational structure in the credit institution or the group, in accordance with the business objectives, strategies and policies approved by the management body. Where the credit institution operates outside the Republic or operates through special purpose vehicles or other structures or in jurisdictions that impede transparency, the senior management shall exercise adequate oversight of the credit institution's group-wide operations, including such operations and ensure that appropriate reporting structures are put in place and that all material information concerning non-transparent or non-standard structures, foreign branches and subsidiaries outside the Republic is accessible to the management body and to the supervisory authorities.

(2) Senior management is responsible for delegating duties to the staff and establishing a management structure and hierarchy that promotes accountability and transparency without gaps in reporting lines and shall oversee the exercise of such delegated responsibility.

(3) Senior management shall implement effective capital and funding and liquidity planning and budget process consistent with the direction given by the management body; the senior management shall monitor the budget implementation and funding and liquidity process, identify weaknesses and potential limitations and evaluate them for materiality, and develop recovery plans for any weaknesses affecting the adequacy of funding and own funds.

(4) Senior management shall set the proper tone and example in implementing the code of business conduct and corporate values and instilling a culture where staff are encouraged to identify ethical, compliance or risk issues as opposed to relying on internal control functions to identify them, consistent with the direction given by the management body and in accordance with the provisions of this Directive.

(5) Senior management shall implement an appropriate compliance framework consistent with the direction given by the management body and in accordance with Part 9 of this Directive.

(6) Senior management shall implement an appropriate risk management framework consistent with the risk strategy and appetite and direction given by the management body and in accordance with Part 9 of this Directive; senior management shall ensure that a new products approval policy is developed and effectively implemented in accordance with paragraph 58 of this Directive.

(7) Senior management shall implement an appropriate internal control framework consistent with the direction given by the management body and in accordance with 9 of this Directive. the senior management shall ensure that sufficient resources with appropriate authority and expertise are dedicated to internal control functions.

(8) Senior management shall ensure that the credit institution develops appropriate information and communication systems to help the management body and senior management to provide effective oversight of the credit institution consistent with the direction given by the management body and in accordance with Part 11 of this Directive. Senior management shall be responsible for ensuring that appropriate records are kept.

(9) Senior management shall set appropriate human resource policies including management development and succession planning.

(10) Credit institutions shall ensure the adequate physical presence of senior management in the performance of their duties as defined by this Directive and in compliance with applicable laws and regulations.

Providing the management body with recommendations.

29.- (1) Senior management shall make informed recommendations to the management body about the business objectives, risk strategy and risk appetite, capital and funding plans and distribution decisions and remuneration policy.

(2) Senior management shall ensure that proposed recommendations have sufficient analytical support and fully reflect the expectations of important stakeholders, including creditors, counterparties, investors, and supervisory authorities.

(3) Senior management shall report to the management body weaknesses and identified limitations of strategies and plans with remediation recommendations.

PART 5 - REMUNERATION FRAMEWORK

Remuneration policies. EBA/GL/2015/22 21.12.2015.

30.- (1) Credit institutions shall comply with the EBA Guidelines on sound remuneration policies pursuant to Article 74 (3) and Article 75 (2) of Directive 2013/36/EU and disclosures under Article 450 of Regulation (EU) No 575/2013.

(2) When establishing and applying the total remuneration policies, inclusive of salaries and discretionary pension benefits, for categories of staff, whose professional activities have a material

impact on the credit institution's risk profile, credit institutions shall comply with the following requirements in a manner that is appropriate to their size, internal organisation and the nature, scope and complexity of their activities:

(a) the remuneration policy is consistent with and promotes sound and effective risk management and does not encourage risk-taking that exceeds the level of tolerated risk of the credit institution;

(b) the remuneration policy is a gender neutral remuneration policy;

(c) the remuneration policy is in line with the business strategy, objectives, values and long-term interests of the credit institution, and incorporates measures to avoid conflicts of interest;

(d) the management body of the credit institution in its supervisory function adopts and periodically reviews the general principles of the remuneration policy and is responsible for overseeing its implementation;

(e) the implementation of the remuneration policy is, at least annually, subject to central and independent internal review for compliance with policies and procedures for remuneration adopted by the management body in its supervisory function;

(f) staff engaged in internal control functions are independent from the business units they oversee, have appropriate authority, and are remunerated in accordance with the achievement of the objectives linked to their functions, independent of the performance of the business areas they control;

(g) the remuneration of the senior officers in the risk management and compliance functions is directly overseen by the remuneration committee or by a combined nomination and remuneration committee if it has been authorised by the competent authority in accordance with subparagraph (1) of paragraph 24 of this Directive;

(h) the remuneration policy, taking into account national criteria on wage setting, makes a clear distinction between criteria for setting:

(i) basic fixed remuneration, which shall primarily reflect relevant professional experience and organisational responsibility as set out in an employee's job description as part of the terms of employment; and

(ii) variable remuneration which shall reflect a sustainable and risk adjusted performance as well as performance in excess of that required to fulfil the employee's job description as part of the terms of employment.

(3) For the purposes of sub-paragraph 2, the categories of staff whose professional activities have a material impact on the risk profile of credit institutions shall include at least:

(a) all of the members of the management body and the senior management,

(b) the staff members with managerial responsibility over the credit institution's control functions or material business units,

(c) the staff members who were entitled to significant remuneration in the preceding financial year, provided that the following conditions are met:

(i) the staff member's remuneration is equal to or greater than five hundred thousand (500,000) euros and equal to or greater than the average remuneration awarded to the members of the management body and to the senior management of the credit institution referred to in point (a),

(ii) the staff member performs professional activity within a material business unit and the activity is of a kind that has a significant impact on the relevant business unit's risk profile.

(4) Credit institutions shall ensure that shareholders are informed of the total remuneration of senior management.

Variable elements of remuneration.

31.- (1) For variable elements of remuneration, the following principles shall apply in addition to, and under the same conditions as, those set out in paragraph 30 of this Directive:

(a) where remuneration is performance related, the total amount of remuneration is based on a combination of the assessment of the performance of the individual and of the business unit concerned and of the overall results of the credit institution and when assessing individual performance, financial and non-financial criteria are taken into account;

(b) the assessment of the performance is set in a multi-year framework in order to ensure that the assessment process is based on longer-term performance and that the actual payment of performance-based components of remuneration is spread over a period which takes account of the underlying business cycle of the credit institution and its business risks;

(c) the total variable remuneration does not limit the ability of the credit institution to strengthen its capital base;

(d) guaranteed variable remuneration is not consistent with sound risk management or the pay-for-performance principle and shall not be a part of prospective remuneration plans;

(e) guaranteed variable remuneration is exceptional, occurs only when hiring new staff and where the credit institution has a sound and strong capital base and is limited to the first year of employment;

(f) fixed and variable components of total remuneration are appropriately balanced and the fixed component represents a sufficiently high proportion of the total remuneration to allow the operation of a fully flexible policy on variable remuneration components, including the possibility to pay no variable remuneration component;

(g) credit institutions shall set the appropriate ratios between the fixed and the variable component of the total remuneration, whereby the following principles shall apply:

(i) the variable component shall not exceed fifty percent (50%) of the fixed component of the total remuneration for each individual;

(ii) shareholders or owners or members of the credit institution may approve a higher maximum level of the ratio between the fixed and variable components of remuneration provided the overall level of the variable component shall not exceed one hundred percent (100%) of the fixed component of the total remuneration for each individual; any approval of a higher ratio in accordance with the first subparagraph of this point shall be carried out in accordance with the following procedure:

(A) the shareholders or owners or members of the credit institution shall act upon a detailed recommendation by the credit institution giving the reasons for, and the scope of, an approval sought, including the number of staff affected, their functions and the expected impact on the requirement to maintain a sound capital base;

(B) shareholders or owners or members of the credit institution shall act by a majority of at least sixty six percent (66%) provided that at least fifty percent (50%) of the shares or equivalent ownership rights are represented or, failing that, shall act by a majority of seventy five percent (75%) of the ownership rights represented;

(C) the credit institution shall notify all shareholders or owners or members of the credit institution, providing a reasonable notice period in advance, that an approval under point (a) above;

(D) the credit institution shall, without delay, inform the competent authority of the recommendation to its shareholders or owners or members, including the proposed higher maximum ratio and the reasons therefore and shall be able to demonstrate to the competent authority that the proposed higher ratio does not conflict with the credit institution's obligations under this Directive and under Regulation (EU) No 575/2013, having regard in particular to the credit institution's own funds obligations;

(E) the credit institution shall, without delay, inform the competent authority of the decisions taken by its shareholders or owners or members, including any approved higher maximum ratio pursuant to point (a) above, and the competent authority shall use the information received to benchmark the practices of credit institutions in that regard;

(F) staff who are directly concerned by the higher maximum levels of variable remuneration referred to in this point shall not, where applicable, be allowed to exercise, directly or indirectly, any voting rights they may have as shareholders or owners or members of the credit institution;

(iii) credit institutions may apply a discount rate to a maximum of twenty five percent (25%) of total variable remuneration provided it is paid in instruments that are deferred for a period of not less than five (5) years. Credit institutions that opt to apply the provisions of this point, shall comply with the EBA Guidelines on the Applicable Notional Discount Rate for Variable Remuneration of 2014;

EBA/GL/2014/01
27.03.2014.

(h) payments relating to the early termination of a contract reflect performance achieved over time and do not reward failure or misconduct;

(i) remuneration packages relating to compensation or buy out from contracts in previous employment shall align with the long-term interests of the credit institution including retention, deferral, performance and clawback arrangements;

(j) the measurement of performance used to calculate variable remuneration components or pools of variable remuneration components includes an adjustment for all types of current and future risks and takes into account the cost of the capital and the liquidity required;

(k) the allocation of the variable remuneration components within the credit institution shall also take into account all types of current and future risks;

(l) a substantial portion, and in any event at least fifty percent (50%), of any variable remuneration shall consist of a balance of the following:

(i) shares or equivalent ownership interests, or share- linked instruments or equivalent non-cash instruments, subject to the legal structure of the credit institution concerned;

(ii) where possible, other instruments within the meaning of Article 52 or 63 of Regulation (EU) No 575/2013 or other instruments which can be fully converted to Common Equity Tier 1 instruments or written down, that in each case adequately reflect the credit quality of the credit institution as a going concern and are appropriate to be used for the purposes of variable remuneration.

The instruments referred to in this point shall be subject to an appropriate retention policy designed to align incentives with the longer-term interests of the credit institution. The competent authority may place restrictions on the types and designs of those instruments or prohibit certain instruments as appropriate. This point shall be applied to both the portion of the variable remuneration component deferred in accordance with point (m) and the portion of the variable remuneration component not deferred;

(m) (i) a substantial portion, and in any event at least forty percent (40%), of the variable remuneration component is deferred over a period which is not less than three (3) to five (5) years and is correctly aligned with the nature of the business, its risks and the activities of the staff member concerned. For members of the management body and senior management of credit institutions that are significant in terms of size, internal organisation and nature, scope and complexity of their activities, the deferral period shall not be less than five (5) years.

(ii) Remuneration payable under deferral arrangements shall vest no faster than on a pro-rata basis. In the case of a variable remuneration component of a particularly high amount, at least sixty percent (60%) of the amount shall be deferred. The length of the deferral period shall be established in accordance with the business cycle, the nature of the business, its risks and the activities of the staff member concerned;

(n) the variable remuneration, including the deferred portion, is paid or vests only if it is sustainable according to the financial situation of the credit institution as a whole, and justified on the basis of the performance of the credit institution, the business unit and the individual concerned.

Without prejudice to the general principles of national contract and labour law, the total variable remuneration shall generally be considerably contracted where subdued or negative financial performance of the credit institution occurs, taking into account both current remuneration and reductions in pay-outs of amounts previously earned, including through malus or clawback arrangements.

Up to one hundred per cent (100%) of the total variable remuneration shall be subject to malus or clawback arrangements. Institutions shall set specific criteria for the application of malus and clawback. Such criteria shall in particular cover situations where the staff member:

(i) participated in or was responsible for conduct which resulted in significant losses to the credit institution;

(ii) failed to meet appropriate standards of fitness and propriety;

(o) the pension policy is in line with the business strategy, objectives, values and long-term interests of the credit institution.

If the employee leaves the credit institution before retirement, discretionary pension benefits shall be held by the credit institution for a period of five years in the form of instruments referred to in point ιβ). Where an employee reaches retirement, discretionary pension benefits shall be paid to the employee in the form of instruments referred to in point (l) subject to a five-year retention period;

(p) staff members are required to undertake not to use personal hedging strategies or remuneration- and liability- related insurance to undermine the risk alignment effects embedded in their remuneration arrangements;

(q) variable remuneration is not paid through vehicles or methods that facilitate the non-compliance with this Directive or Regulation (EU) No 575/2013.

(2) By way of derogation from subparagraph 1, the requirements foreseen in points (l) and (m) and in the second paragraph of point (o) of that sub-paragraph shall not apply to:

(a) a credit institution which is not a large credit institution as defined in point (146) of Article 4 paragraph 1 of Regulation (EU) No 575/2013 and the value of its assets is on average and on an individual basis in accordance with this Directive and Regulation (EU) No 575/2013 equal to or less than five (5) billion euros during the four years immediately preceding the current financial year,

(b) a staff member whose annual variable remuneration does not exceed fifty thousand (50,000) euros and does not represent more than one third of the staff member’s total annual remuneration.

(3) By way of derogation from subparagraph 2 (a) of this paragraph, the competent authority may lower or increase the ceiling referred to in that provision, provided that:

(a) the said credit institution is not a large credit institution, as defined in point (146) of Article 4 paragraph 1 of Regulation (EU) 575/2013 and where the threshold is increased:

(i) the credit institution meets the criteria set out in points (145) (c), (d) and (e) of Article 4 (1) of Regulation (EU) 575/2013; and

(ii) the threshold does not exceed fifteen billion (15,000,000,000) euros,

(b) it is appropriate to modify the ceiling, in accordance with this paragraph, taking into account the nature, scope and complexity of the activities of the credit institution, its internal organisation or, where appropriate, the characteristics of the group to which it belongs.

(4) By way of derogation from subparagraph 2 (b) of this paragraph, the competent authority may decide that staff members entitled to annual variable remuneration below the threshold and share referred to in that item are not be subject to the exception set out in that paragraph, because of the specificities of the national market in terms of remuneration practices or because of the nature of the responsibilities and job profile of those staff members.

Credit institutions that benefit from government intervention.

32.- In the case of credit institutions that benefit from exceptional government intervention, the following principles shall apply in addition to those set out in sub-paragraph (2) of paragraph 30 of this Directive:

(a) variable remuneration is strictly limited as a percentage of net revenue, where it is inconsistent with the maintenance of a sound capital base and timely exit from government support;

(b) remuneration is restructured by credit institutions in a manner aligned with sound risk management and long-term growth, including, where appropriate, establishing limits to the remuneration of the members of the management body of the credit institution;

(c) no variable remuneration is paid to members of the management body of the credit institution unless justified.

PART 6 – GOVERNANCE FRAMEWORK

Organisational framework.

33.- (1) The management body of a credit institution shall ensure a suitable and transparent organisational and operational structure for that credit institution and shall have a written description thereof.

(2) The structure shall promote and demonstrate the effective and prudent management of a credit institution at individual, sub-consolidated and consolidated levels.

(3) The management body shall ensure that the internal control functions are independent of the business lines they control, including that there is an adequate segregation of duties, and that they have the appropriate financial and human resources as well as powers to effectively perform their role.

(4) The reporting lines and the allocation of responsibilities, in particular among key function holders, within a credit institution shall be clear, well-defined, coherent, enforceable and duly documented. The documentation shall be updated as appropriate.

(5) The structure of the credit institution shall not impede the ability of the management body to oversee and manage effectively the risks the credit institution or the group faces or the ability of the competent authority to effectively supervise the credit institution.

(6) The management body shall assess whether and how material changes to the group's structure (for instance, setting up of new subsidiaries, mergers and acquisitions, selling or winding-up parts of the group, or external developments) impact on the soundness of the credit institution's organisational framework. Where weaknesses are identified, the management body shall make any necessary adjustments swiftly.

Know your structure.

34.- (1) The management body shall fully know and understand the legal, organisational and operational structure of the credit institution ('know your structure') and ensure that it is in line with its approved business and risk strategy and risk appetite.

(2) The management body shall be responsible for the approval of sound strategies and policies for the establishment of new structures.

(3) Where a credit institution creates many legal entities within its group, their number and, in particular, the interconnections and transactions between them shall not pose challenges for the design of its internal governance, and for the effective management and oversight of the risks of the group as a whole.

(4) The management body shall ensure that the structure of a credit institution and, where applicable, the structures within a group, taking into account the criteria specified in paragraph 36 of this Directive, are clear, efficient and transparent to the credit institution's staff, shareholders and other stakeholders and to the competent authority.

(5) The management body shall guide the credit institution's structure, its evolution and its limitations and shall ensure that the structure is justified and efficient and does not involve undue or inappropriate complexity.

(6) (a) The management body of a consolidating credit institution shall understand not only the legal, organisational and operational structure of the group but also the purpose and activities of its different entities and the links and relationships among them. This includes understanding group-specific operational risks and intra-group exposures as well as how the group's funding, capital, liquidity and risk profiles could be affected under normal and adverse circumstances.

(b) The management body shall ensure that the credit institution is able to produce information on the group in a timely manner, regarding the type, the characteristics, the organisational chart, the ownership structure and the businesses of each legal entity, and that the credit institutions within the group comply with all supervisory reporting requirements on an individual, sub-consolidated and consolidated basis.

(7) (a) The management body of a consolidating credit institution shall ensure that the different group entities (including the consolidating credit institution itself) receive enough information to get a clear perception of the general objectives, strategies and risk profile of the group and how the group entity concerned is embedded in the group's structure and operational functioning. Such information and revisions thereof shall be documented and made available to the relevant functions concerned, including the management body, business lines and internal control functions.

(b) The members of the management body of a consolidating credit institution shall keep themselves informed about the risks the group's structure causes, taking into account the criteria specified in paragraph 36 of this Directive.

(c) The information referred to in points (a) and (b) includes receiving:

(i) information on major risk drivers;

(ii) regular reports assessing the credit institution's overall structure and evaluating the compliance of individual entities' activities with the approved group-wide strategy; and

(iii) regular reports on topics where the regulatory framework requires compliance at individual, sub-consolidated and consolidated levels.

Complex structures and non-standard or non- transparent activities.

35.- (1) Credit institutions shall avoid setting up complex and potentially non-transparent structures.

(2) shall take into account in their decision-making the results of a risk assessment performed to identify whether such structures could be used for a purpose connected with money laundering or other financial crimes and the respective controls and legal framework in place.

(3) For the purposes of sub-paragraph (2), credit institutions shall take into account at least:

(a) the extent to which the jurisdiction in which the structure will be set up complies effectively with EU and international standards on tax transparency, anti-money laundering and countering the financing of terrorism;

(b) the extent to which the structure serves an obvious economic and lawful purpose;

(c) the extent to which the structure could be used to hide the identity of the ultimate beneficial owner;

(d) the extent to which the customer's request that leads to the possible setting up of a structure gives rise to concern;

(e) whether the structure might impede appropriate oversight by the credit institution's management body or the credit institution's ability to manage the related risk; and

(f) whether the structure poses obstacles to effective supervision by the competent authority.

(4) In any case, credit institutions shall not set up opaque or unnecessarily complex structures which have no clear economic rationale or legal purpose or if credit institutions are concerned that these structures might be used for a purpose connected with financial crime.

(5) When setting up such structures, the management body shall understand them and their purpose and the particular risks associated with them and ensure that the internal control functions are appropriately involved.

(6) Such structures shall be approved and maintained only when their purpose has been clearly defined and understood, and when the management body is satisfied that all material risks, including reputational risks, have been identified, that all risks can be managed effectively and appropriately reported, and that effective oversight has been ensured. The more complex and opaque the organisational and operational structure and the greater the risks, the more intensive the oversight of the structure shall be by the management body.

(7) Credit institutions shall document their decisions and be able to justify their decisions to the competent authority.

(8) The management body shall ensure that appropriate actions are taken to avoid or mitigate the risks of activities within such structures. This includes ensuring that:

(a) the credit institution has in place adequate policies and procedures and documented processes (for instance applicable limits, information requirements) for the consideration, compliance, approval and risk management of such activities, taking into account the consequences for the group's organisational and operational structure, its risk profile and its reputational risk;

(b) information concerning these activities and the risks thereof is accessible to the consolidating credit institution and internal and external auditors and is reported to the management body in its supervisory function and to the competent authority that granted authorisation; and

(c) the credit institution periodically assesses the continuing need to maintain such structures.

(9) The structures and activities of the credit institution, including their compliance with legislation and professional standards, shall be subject to regular review by the internal audit function following a risk- based approach.

(10) Credit institutions shall take the same risk management measures as for the credit institution's own business activities when they perform non-standard or non-transparent activities for clients (for instance helping clients to set up vehicles in offshore jurisdictions, developing complex structures, financing transactions for them or providing trustee services) that pose similar internal governance challenges and create significant operational and reputational risks. In particular, credit institutions shall analyse the reason why a client wants to set up a particular structure.

Organisational framework in a group context.

36.- (1) For the purposes of paragraph 2 of this Directive, and subject to the provisions of subsections 4 and 5 of section 19F of the Law, parent undertakings and subsidiaries within the scope of prudential consolidation shall ensure that governance arrangements, processes and mechanisms and applied in their in their subsidiaries not subject to the provisions of the Law and of the Directives, including those located in third countries and offshore financial centres in order to ensure robust governance arrangements on a consolidated and sub-consolidated basis.

(2) Competent functions within the consolidating credit institution and its subsidiaries shall interact and exchange data and information as appropriate. The governance arrangements, processes and mechanisms shall ensure that the consolidating credit institution has sufficient data and information and is able to assess the group-wide risk profile, as detailed in in paragraph 34 of this Directive.

(3) The management body of a subsidiary that is subject to the provisions of the Law, of this Directive or Directive 2013/36/EU shall adopt and implement on the individual level the group-wide governance policies established at the consolidated or sub-consolidated level, in a manner that complies with all specific requirements under EU and national law.

(4) At the consolidated and sub-consolidated levels, the consolidating credit institution shall ensure adherence to the group-wide governance policies by all credit institutions and other entities within the scope of prudential consolidation, including their subsidiaries not themselves subject to the provisions of the Law and of this Directive.

(5) When implementing governance policies, the consolidating credit institution shall ensure that robust governance arrangements are in place for each subsidiary and consider specific arrangements, processes and mechanisms where business activities are organised not in separate legal entities but within a matrix of business lines that encompasses multiple legal entities.

(6) A consolidating credit institution shall consider the interests of all its subsidiaries, and how strategies and policies contribute to the interest of each subsidiary and the interest of the group as a whole over the long term.

(7) Parent undertakings and their subsidiaries shall ensure that the credit institutions and entities within the group comply with all specific requirements in any relevant jurisdiction.

(8) The consolidating credit institution shall ensure that subsidiaries established in third countries, and which are included in the scope of prudential consolidation, have governance arrangements, processes and mechanisms in place that are consistent with group-wide governance policies and comply with the requirements of paragraphs (2), (3) and (5) of section 19, of section 19B, of section 19C, of section 19D, of section 22E, of section 24A, of section 24B, of paragraphs 13 and 14 of section 26, of paragraphs (1) and (2) of section 26C, of section 26D and of paragraph (1) of section

30B of the Law, the provisions of the Assessment of Suitability of the Members of the Management Body and Key Function Holders of Authorised Credit institutions of 2020, as well as the provisions of this Directive, as long as this is not unlawful under the laws of the third country.

(9) (a) The governance requirements foreseen by the Law and by this Directive apply to credit institutions under paragraph 3 of this Directive, independent of the fact that they may be subsidiaries of a parent undertaking in a third country.

(b) Where a credit institution is a subsidiary of a parent undertaking in a third country and the credit institution constitutes a credit institution required to consolidate, the scope of prudential consolidation does not include the level of the parent undertaking located in a third country and other direct subsidiaries of that parent undertaking.

(c) The consolidating credit institution shall ensure that the group-wide governance policy of the parent credit institution in a third country is taken into consideration within its own, governance policy insofar as this is not contrary to the requirements set out under relevant EU law, including Directive 2013/36/EU, the Law, and this Directive.

Annex I

(10) When establishing policies and documenting governance arrangements, credit institutions shall take into account the aspects listed in Annex I of this Directive. While policies and documentation may be included in separate documents, credit institutions shall consider combining them or referring to them in a single governance framework document.

PART 7 – OUTSOURCING TO THIRD PARTIES

Outsourcing policy.

37.- (1) The management body shall approve and regularly review and update the outsourcing policy of a credit institution, ensuring that appropriate changes are implemented in a timely manner, and in any event at least every three years, the written outsourcing policy of the credit institution, ensuring the timely implementation of appropriate changes.

(2) (a) The outsourcing policy shall consider the impact of outsourcing on a credit institution's business and the risks it faces (such as operational risks, including legal and IT and security Risks, reputational risks and concentration risks.

(b) The policy shall include the reporting and monitoring arrangements to be implemented from inception to the end of an outsourcing agreement including drawing up the business case for outsourcing, entering into an outsourcing contract, the implementation of the contract to its expiry, contingency plans and exit strategies.

(c) the credit institution shall remain fully responsible for all outsourced services and activities and management decisions arising from them. Accordingly, the outsourcing policy shall make it clear that outsourcing does not relieve the credit institution of its regulatory obligations and its responsibilities to its customers.

(3) The policy shall state that outsourcing arrangements shall not hinder effective on-site or off-site supervision of the credit institution and shall not contravene any supervisory restrictions on services and activities. The policy shall also cover intragroup outsourcing (i.e., services provided by a separate legal entity within a credit institution's group) and take into account any specific group circumstances.

Outsourcing procedures.
EBA/GL/2019/02
25.02.2019.

38.- (1) Credit institutions shall apply the EBA Guidelines on outsourcing arrangements in relation to their outsourcing policy and processes.

(2) Credit institutions shall clearly assign responsibilities for the documentation, management and control of outsourcing agreements and shall allocate adequate resources in order to ensure compliance with all legislative and regulatory requirements, including the EBA Guidelines referred to in sub-paragraph (1) as well as the documentation and monitoring of all outsourcing agreements.

(3) Taking into account the principle of proportionality, credit institutions shall establish an outsourcing function and, in any event, designate a staff member (Outsourcing Officer) responsible for managing and overseeing the risks of outsourcing agreements as part of the credit institution's internal control framework, as well as for overseeing the documentation of outsourcing agreements. In case the outsourcing Officer is not a member of the management body or an already key function holder, he shall be classified as a the key function holder that falls under the requirements prescribed by the Directive on the Assessment of Suitability of the Members of the Management Body and Key Function Holders of Authorised Credit institutions of 2020.

(4) Within the scope of his duties, the Outsourcing Officer shall liaise with the competent authority for the outsourcing matters and shall provide all the necessary information required by the competent authority.

(5) Credit institutions shall maintain an up-to-date information register on all outsourcing agreements in accordance with the provisions of the EBA Guidelines referred to in sub-paragraph (1) and shall

submit the register to the competent authority, when requested, either in whole or in parts thereof concerning the outsourcing of specific services or activities.

(6) Credit institutions shall submit a report to the competent authority on an annual basis, which shall include the following information concerning the outsourced activities or services that are not considered to be critical or important:

(a) a list of outsourcing arrangements made during the reporting period with a brief description of the relevant service or activity, the duration of the outsourcing arrangement and the relevant owner department / unit of the institution;

(b) the full name and country of establishment of the outsourcing service provider and in the case of a regulated entity, its competent supervisory authority;

(c) a confirmation that a proper assessment of outsourcing risks has been performed;

(d) a confirmation that a formal approval for outsourcing arrangement has been obtained by the relevant authorisation unit; and

(e) a confirmation that a formal legal opinion has been obtained, ascertaining that the outsourced service or activity is not considered critical or important.

The annual report shall be submitted by the 31st of January of each year, with a reference period of the preceding year. The submission date and the reference period may be amended on a case-by-case basis, in agreement with the competent authority.

(7) (a) Credit institutions shall consider that a service or activity is critical or important, inter alia, in the cases listed in the relevant provisions of the EBA Guidelines on outsourcing arrangements.

(b) In addition to the list of cases referred to in point (a), the administration of the credit institution's main information systems by third parties, including the systems that store customer and bank account data, as well as the systems that constitute the source of information for the purpose of reporting on supervisory and accounting matters, are considered to be "critical or important services or activities". It is provided that the use of cloud service providers for the purpose of performing the above tasks is also considered critical or important.

(8) Credit institutions shall obtain, for any outsourcing service or activity, a formal legal opinion regarding whether the service or activity may be considered critical or important or not, in accordance with the provisions of this Directive and the relevant criteria provided by the EBA Guidelines referred to in sub-paragraph (1). The legal opinion is required, notwithstanding the obligation of the credit institution to assess the risks and other factors that should be taken into account for the assessment of each outsourcing arrangement, but it may take into consideration the outcomes of the assessment of these factors.

(9) Credit institutions shall inform the competent authority in writing of any case of outsourcing activity that is deemed critical or important, at least two months before the outsourcing arrangement is finalised, by submitting at least the following information:

(a) the owner department / unit of the institution;

(b) a description of the service or activity that will be outsourced;

(c) information about the outsourcing service provider. If the service provider is supervised by another competent authority, relevant information shall be provided;

(d) a confirmation that the outsourcing arrangement is in accordance with the provisions of this Directive and the EBA Guidelines on outsourcing arrangements, including a confirmation that a risk assessment has been carried out by the risk management function and that a legal opinion has been obtained;

(e) confirmation that formal approval for the outsourcing arrangement has been obtained by the relevant authorisation unit; and

(f) a confirmation that a formal outsourcing agreement will be prepared and signed between the credit institution and the service provider, which shall be in full compliance with the provisions of this Directive and the EBA Guidelines referred to in sub-paragraph (1).

(10) Within the period of two months referred to in sub-paragraph (9):

(a) the competent authority may request further information on the outsourcing arrangement of a critical or important activity and/or in case of deficiencies, it may require the adoption of appropriate corrective measures. In such a case, the credit institution shall not proceed with the outsourcing arrangement before the competent authority is satisfied with the above and informs the credit institution in writing in this respect.

(b) the competent authority may object to the outsourcing arrangement, by justifying its decision in this regard. In such a case, the credit institution shall not proceed with such outsourcing arrangement.

PART 8 - RISK CULTURE AND BUSINESS CONDUCT

Risk culture.

39.- (1) A sound, diligent and consistent risk culture shall be a key element of credit institutions' effective risk management and shall enable credit institutions to make sound and informed decisions.

(2) Credit institutions shall develop an integrated and credit institution-wide risk culture, based on a full understanding and holistic view of the risks they face and how they are managed, taking into account the credit institution's risk appetite.

(3) Credit institutions shall develop a risk culture through policies, communication and staff training regarding the credit institutions' activities, strategy and risk profile, and shall adapt communication and staff training to take into account staff's responsibilities regarding risk-taking and risk management.

(4) Staff shall be fully aware of their responsibilities relating to risk management. Risk management shall not be confined to risk specialists or internal control functions. Business units, under the oversight of the management body, shall be primarily responsible for managing risks on a day-to-day basis in line with the credit institution's policies, procedures and controls, taking into account the credit institution's risk appetite and risk capacity.

(5) A strong risk culture shall include but is not necessarily limited to:

(a) Tone from the top: the management body shall be responsible for setting and communicating the credit institution's core values and expectations. The conduct of its members shall reflect the values being espoused. Credit institutions' management, including key function holders, shall contribute to the internal communication of core values and expectations to staff. Staff shall act in accordance with all applicable laws and regulations and promptly escalate observed non-compliance. The management body shall on an ongoing basis promote, monitor and assess the risk culture of the credit institution; consider the impact of the risk culture on the financial stability, risk profile and robust governance of the credit institution; and make changes where necessary.

(b) Accountability: relevant staff at all levels shall know and understand the core values of the credit institution and, to the extent necessary for their role, its risk appetite and risk capacity. They shall be capable of performing their roles and be aware that they will be held accountable for their actions in relation to the credit institution's risk-taking conduct.

(c) Effective communication and challenge: a sound risk culture shall promote an environment of open communication and effective challenge in which decision-making processes encourage a broad range of views, allow for testing of current practices, stimulate a constructive critical attitude among staff, and promote an environment of open and constructive engagement throughout the entire organisation.

(d) Incentives: appropriate incentives shall play a key role in aligning risk-taking conduct with the credit institution's risk profile and its long-term interest.

Corporate values and code of conduct.

40.- (1) The management body shall develop, adopt, adhere to and promote high ethical and professional standards, taking into account the specific needs and characteristics of the credit institution, and shall ensure the implementation of such standards, through a code of conduct or similar instrument.

(2) The management body shall also oversee adherence to the standards referred to in sub-paragraph (1) by staff. Where applicable, the management body may adopt and implement the credit institution's group-wide standards or common standards released by associations or other relevant organisations.

(3) Credit institutions shall ensure that there is no discrimination on the basis of gender, race, colour, ethnic origin or social origin, genetic characteristics, language, religion or belief, political or otherwise, membership of a national minority, property, birth, disability, age, or sexual orientation.

(4) The policies of a credit institution shall be gender neutral and credit institutions shall implement measures that ensure equal opportunities for all genders, including career prospects, and aim to improve the under-representation of under-represented gender in management positions. and

members of staff holding managerial responsibilities as defined in Commission Delegated Regulation (EU) 2019/923. Credit institutions shall monitor the development of the gender pay gap separately for the identified staff (excluding members of the management body). Credit institutions shall have policies that facilitate the reintegration of staff after maternity, paternity, or parental leave.

(5) The implemented standards shall aim at enhancing the credit institution's robust government arrangements and reducing the risks to which the credit institution is exposed, in particular operational and reputational risks, which can have a considerable adverse impact on a credit institution's profitability and sustainability through fines, litigation costs, restrictions imposed by competent authorities, other financial and criminal penalties, and the loss of brand value and consumer confidence.

(6) The management body shall have clear and documented policies for how these standards shall be met. These policies shall:

(a) remind staff that all the credit institution's activities shall be conducted in compliance with the applicable law and with the credit institution's corporate values;

(b) promote risk awareness through a strong risk culture in line with paragraph 39 of this Directive, conveying the management body's expectation that activities will not go beyond the defined risk appetite and limits defined by the credit institution and the respective responsibilities of staff;

(c) set out principles on and provide examples of acceptable and unacceptable conducts linked in particular to financial misreporting and misconduct, economic and financial crime, including fraud, money laundering and anti-trust practices, financial sanctions, bribery and corruption, market manipulation, mis-selling and other violations of consumer protection laws, tax offenses, whether committed directly or indirectly, and which include unlawful or banned dividend arbitrage schemes;

(d) clarify that, in addition to complying with legal and regulatory requirements and internal policies, staff are expected to behave with honesty and integrity and to perform their duties with due skill, care and diligence; and

(e) ensure that staff are aware of the potential internal and external disciplinary actions, legal actions and sanctions that may follow misconduct and unacceptable behaviours.

(7) Credit institutions shall monitor compliance with such standards and ensure staff awareness, for instance by providing training.

(8) Credit institutions shall define the function responsible for monitoring compliance with and evaluating breaches of the code of conduct or similar instrument and a process for dealing with issues of non-compliance. The results shall periodically be reported to the management body.

Conflict of interest policy at credit institutional level.

41.- (1) The management body shall be responsible for establishing, approving and overseeing the implementation and maintenance of effective policies to identify, assess, manage and mitigate or prevent actual and potential conflicts of interest at credit institutional level, for instance as a result of the various activities and roles of the credit institution, of different credit institutions within the scope of prudential consolidation or of different business lines or units within a credit institution, or with regard to external stakeholders.

(2) Credit institutions shall take, within their organisational and administrative arrangements, adequate measures to prevent conflicts of interest from adversely affecting the interests of its clients.

(3) Credit institutions' measures to manage or where appropriate mitigate conflicts of interest shall be documented and include, inter alia:

(a) an appropriate segregation of duties, for instance, entrusting conflicting activities within the processing of transactions or when providing services to different persons, or entrusting supervisory and reporting responsibilities for conflicting activities to different persons;

(b) establishing information barriers, for instance, through the physical separation of certain business lines or units.

Conflict of interest policy for staff.

42.- (1) The management body shall be responsible for establishing, approving and overseeing the implementation and maintenance of effective policies to identify, assess, manage and mitigate or prevent actual and potential conflicts between the interests of the credit institution and the private interests of staff, including members of the management body, which could adversely influence the performance of their duties and responsibilities. A consolidating credit institution shall consider interests within a group-wide conflict of interest policy on a consolidated or sub-consolidated basis.

(2) (a) The specific policy referred to in sub-paragraph (1) shall aim at identifying conflicts of interest of staff, including the interests of their closest family members.

(b) Credit institutions shall take into consideration that conflicts of interest may arise not only from present but also from past personal or professional relationships.

(c) Where conflicts of interest arise, credit institutions shall assess their materiality and decide on and implement as appropriate mitigating measures.

(3) Regarding conflicts of interest that may result from past relationships, credit institutions shall set an appropriate timeframe for which they want staff to report such conflicts of interest, on the basis that these may still have an impact on staff's conduct and participation in decision-making.

(4) The policy shall cover at least the following situations or relationships where conflicts of interest may arise:

(a) economic interests, for instance, shares, other ownership rights and memberships, financial holdings and other economic interests in commercial customers, intellectual property rights, loans granted by the credit institution to a company owned by staff, membership in a body or ownership of a body or entity with conflicting interests;

(b) personal or professional relationships with the owners of qualifying holdings in the credit institution;

(c) personal or professional relationships with staff of the credit institution or entities included within the scope of prudential consolidation, for instance, family relationships;

(d) other employment and previous employment within the recent past, for instance, five years;

(e) personal or professional relationships with relevant external stakeholders, for instance, being associated with material suppliers, consultancies or other service providers; and

(f) political influence or political relationships.

(5) Notwithstanding the above, credit institutions shall take into consideration that being a shareholder of a credit institution or having private accounts or loans with or using other services of a credit institution shall not lead to a situation where staff are considered to have a conflict of interest if they stay within an appropriate de minimis threshold to be established by credit institutions as part of their policy.

(6) The policy shall set out the processes for reporting and communication to the function responsible under the policy. Staff shall have the duty to promptly disclose internally any matter that may result, or has already resulted, in a conflict of interest.

(7) The policy shall differentiate between conflicts of interest that persist and need to be managed permanently and conflicts of interest that occur unexpectedly with regard to a single event – such as for instance a transaction, the selection of service provider - and can usually be managed with a one-off measure. In all circumstances, the interest of the credit institution shall be central to the decisions taken.

(8) The policy shall set out procedures, measures, documentation requirements and responsibilities for the identification and prevention of conflicts of interest, for the assessment of their materiality and for taking mitigating measures. Such procedures, requirements, responsibilities and measures shall include:

(a) entrusting conflicting activities or transactions to different persons;

(b) preventing staff who are also active outside the credit institution from having inappropriate influence within the credit institution regarding those other activities;

(c) establishing the responsibility of the members of the management body to abstain from voting on any matter where a member has or may have a conflict of interest or where the member's objectivity or ability to properly fulfil duties to the credit institution may be otherwise compromised;

(d) establishing adequate procedures for transactions with related parties (credit institutions may consider, inter alia, requiring transactions to be conducted at arm's length, requiring that all relevant internal control procedures fully apply to such transactions, requiring binding consultative advice from independent members of the management body, requiring the approval by shareholders of the most relevant transactions and limiting exposure to such transactions); and

(e) preventing members of the management body from holding directorships in competing credit institutions, unless they are within credit institutions that belong to the same credit institutional protection scheme, as referred to in Article 113(7) of Regulation (EU) No 575/2013, credit institutions permanently affiliated to a central body, as referred to in Article 10 of Regulation (EU) No 575/2013, or credit institutions within the scope of prudential consolidation.

(9) The policy shall specifically cover the risk of conflicts of interest at the level of the management body and provide sufficient guidance on the identification and management of conflicts of interest that may impede the ability of members of the management body to take objective and impartial decisions that aim to fulfil the best interests of the credit institution. Credit institutions shall take into

consideration that conflicts of interest can have an impact on the independence of mind of members of the management body.

(10) In mitigating conflicts of interest identified for members of the management body, the credit institution shall document the measures taken, including the rationale for how effective they are to ensure objective decision-making.

(11) Actual or potential conflicts of interest that have been disclosed to the responsible function within the credit institution shall be appropriately assessed and managed. If a conflict of interest of staff is identified, the credit institution shall document the decision taken, in particular if the conflict of interest and the related risks have been accepted, and if it has been accepted, how this conflict of interest has been satisfactorily mitigated or remedied.

(12) All actual and potential conflicts of interest at management body level, individually and collectively, shall be adequately documented, communicated to the management body, and discussed, decided on and duly managed by the management body.

(13) The existence of non-performing loans of a key function holder, including its related parties, may raise doubts about the independent and impartial judgment of the key function holder in the performance of his or her duties and constitute a conflict of interest. In order to avoid and quickly manage such situations:

(a) credit institutions shall ensure that persons appointed to key functions do not present, at the time of their appointment, loans belonging to the category of non-performing loans.

(b) credit institutions shall establish appropriate policies and procedures for the handling and rapidly eliminating cases where loans granted by the credit institution to a key function holder, including its related parties, have become non-performing loans following his appointment. For instance, such policies and procedures may include the ordinary reporting of these cases to the audit committee and their relevant monitoring by that committee, the setting of a clear timetable for normalisation, etc.

Internal alert procedures.

43.- (1) Credit institutions shall put in place and maintain appropriate internal alert policies and procedures for staff to report potential or actual breaches of regulatory or internal requirements, including, but not limited to, those of Regulation (EU) No 575/2013, national provisions transposing Directive 2013/36/EU and of this Directive, through a specific, independent and autonomous channel.

Official Journal of the EU: L305, 26.11.2019, p.17.

(2) It shall not be necessary for reporting staff to have evidence of a breach; however, they shall have a sufficient level of certainty that provides sufficient reason to launch an investigation.

(3) Credit institutions shall implement appropriate procedures to ensure that they comply with national legislation harmonising national law with Directive 2019/1937/EU on the protection of persons reporting breaches of EU law.

(4) To avoid conflicts of interest, it shall be possible for staff to report breaches outside regular reporting lines (for instance, through the compliance function, the internal audit function or an independent internal whistleblowing procedure) within the credit institution.

125(I) of 2018.

(5) The alert procedures shall ensure the protection of the personal data of both the person who reports the breach and the natural person who is allegedly responsible for the breach, in accordance with Regulation (EU) 2016/679 and the Law on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data.

(6) The alert procedures shall be made available to all staff within a credit institution.

(7) (a) Information provided by staff through the alert procedures shall, if appropriate, be made available to the management body and other responsible functions defined within the internal alert policy. Where required by the member of staff reporting a breach, the information shall be provided to the management body and other responsible functions in an anonymised way.

(b) Credit institutions may also provide for a whistleblowing process that allows information to be submitted in an anonymised way.

(8) Credit institutions shall ensure that the person reporting the breach is appropriately protected from any negative impact, for instance, retaliation, discrimination or other types of unfair treatment. The credit institution shall ensure that no person under the credit institution’s control engages in victimisation of a person who has reported a breach and shall take appropriate measures against those responsible for any such victimisation.

(9) Credit institutions shall also protect persons who have been reported from any negative effects in case the investigation finds no evidence that justifies taking measures against that person. If measures are taken, the credit institution shall take them in a way that aims to protect the person concerned from unintended negative effects that go beyond the objective of the measure taken.

(10) Internal alert procedures shall:

(a) be documented, for instance in staff handbooks;

(b) provide clear rules that ensure that information on the reporting and the reported persons and the breach are treated confidentially, in accordance with Regulation (EU) 2016/679 and the Law on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, unless disclosure is required under national law in the context of further investigations or subsequent judicial proceedings;

(c) protect staff who raise concerns from being victimised because they have disclosed reportable breaches;

(d) ensure that the potential or actual breaches raised are assessed and escalated, including as appropriate to the relevant competent authority or law enforcement agency;

(e) ensure, where possible, that confirmation of receipt of information is provided to staff who have raised potential or actual breaches;

(f) ensure the tracking of the outcome of an investigation into a reported breach; and

(g) ensure appropriate record keeping.

Reporting to the competent authority.

44.- The staff members of credit institutions shall report to the competent authority relevant potential or actual breaches of regulatory requirements, including, but not limited to, those of Regulation (EU) No 575/2013 and national provisions transposing Directive 2013/36/EU, of the Law and of this Directive, in case such members of staff:

(a) have reason to believe that the use of their internal credit institutions' in-house warning procedures may not be effective; or

(b) consider that, notwithstanding the provisions of paragraph 43 of this Directive, any internal complaint would create a risk of adverse consequences for them; or

(c) consider it appropriate to lodge a complaint with the competent authority immediately, on account of the seriousness of the potential or actual breach, and/or the possible involvement of senior management of the credit institution, or

(d) consider it appropriate to submit the complaint immediately to the competent authority for any other reason which they shall explain to the competent authority in the context of the lodging of their complaint.

PART 9 - RISK MANAGEMENT FRAMEWORK

Section I – Handing of specific risks

Credit risk and counterparty risk.

45.- (1) Credit institutions shall lay down sound and well-defined credit-granting criteria and shall clearly establish the process for approving, amending, renewing, and re-financing credits in accordance with the Directive on Loan Origination Processes and Processes of Reviewing Existing Loans of 2016 to 2020, the Arrears Management Directive of 2015 to 2020, the Central Bank Guidelines and or the European Central Bank Guidelines on credit risk management and the respective EBA Guidelines adopted by the Central Bank which require credit institutions to implement.

R.A.A. 74/2016
O.G. Sch. III(I)
No. 4933
18.03.2016

R.A.A. 259/2016
O.G. Sch. III(I)
No. 4964
16.09.2016

R.A.A. 41/2017,
O.G. Sch. III(I)
No. 4994
03.02.2017

R.A.A. 274/2019
O.G. Sch. III(I)
No. 5177
09.08.2019

R.A.A. 106/2020
O.G. Sch. III(I)
No. 5221
19.03.2020.

(2) Credit institutions shall ensure that:

(a) credit-granting is based on sound and well-defined criteria and that the process for approving, amending, renewing, and re-financing credits is clearly established;

(b) institutions have internal methodologies that enable them to assess the credit risk of exposures to individual obligors, securities or securitisation positions and credit risk at the portfolio level. In particular, internal methodologies shall not rely solely or mechanistically on external credit ratings. Where own funds requirements are based on a rating by an External Credit Assessment Institution (ECAI) or based on the fact that an exposure is unrated, this shall not exempt institutions from additionally considering other relevant information for assessing their allocation of internal capital;

(c) the ongoing administration and monitoring of the various credit risk-bearing portfolios and exposures of institutions, including for identifying and managing problem credits and for making adequate value adjustments and provisions, is operated through effective systems;

(d) diversification of credit portfolios is adequate given an institution's target markets and overall credit strategy.

Residual risk.

46.- Credit institutions shall ensure that the risk that recognised credit risk mitigation techniques used are proven to be less effective than expected, is addressed and controlled including by means of written policies and procedures.

Concentration risk.

47.- Credit institutions shall ensure that the concentration risk arising from exposures to each counterparty including central counterparties, groups of connected counterparties and counterparties in the same economic sector, geographic region or from the same activity or commodity, or the application of credit risk mitigation techniques, and in particular risks associated with large indirect credit exposures such as a single collateral issuer, are addressed and controlled including by means of written policies and procedures.

Securitisation risk.

48.- (1) Credit institutions shall evaluate and address through appropriate policies and procedures, the risks arising from securitisation transactions in relation to which a credit institution is investor, originator or sponsor, including reputational risks, such as arise in relation to complex structures or products, in order to ensure that the economic substance of the transaction is fully reflected in the risk assessment and management decisions.

(2) A credit institution which is an originator of a revolving securitisation transaction involving early amortisation provisions shall have liquidity plans to address the implications of both scheduled and early amortisation.

Market risk.

49.- (1) Credit institutions shall implement policies and processes for the identification, measurement and management of all material sources and effects of market risks in line with the guidelines of the Central Bank of management of market risk.

(2) Credit institutions shall take measures so that where the short position falls due before the long position, they also take measures against the risk of a shortage of liquidity.

(3) Credit institutions shall implement policies and processes to ensure that the internal capital is adequate for material market risks that are not subject to an own funds requirement.

(4) Credit institutions which have, in calculating own funds requirements for position risk in accordance with Part Three, Title IV, Chapter 2 of the Regulation (EU) No 575/2013, netted off their positions in one or more of the equities constituting a stock-index against one or more positions in the stock-index future or other stock-index product, shall have adequate internal capital to cover the basis risk of loss caused by the future's or other product's value not moving fully in line with that of its constituent equities; Credit institutions shall also have such adequate internal capital where they hold opposite positions in stock-index futures which are not identical in respect of either their maturity or their composition or both.

(5) Credit institutions shall ensure that, when using the treatment in Article 345 of the Regulation (EU) No 575/2013, they hold sufficient internal capital against the risk of loss which exists between the time of the initial commitment and the following working day.

Interest risk arising from non-trading book activities.

50.- (1) Credit institutions shall implement internal systems and use the standard methodology or simplified standard methodology to identify, evaluate, manage and mitigate the risks arising from potential changes in interest rates that affect both the financial value of the shares and the net interest income from non-trading activities of the credit institution.

(2) Credit institutions shall implement systems to assess and monitor the risks arising from potential changes in credit spreads that affect both the economic value of equity and the net interest income of a credit institution's non-trading book activities..

(3) The competent authority may require a credit institution to use the standard methodology referred to in sub-paragraph (1) where the internal systems applied by that credit institution for the purpose of evaluating the risks referred to in that subparagraph are not satisfactory.

(4) The competent authority may require a small and non-complex credit institution as defined in point (145) of Article 4 paragraph 1 of Regulation (EU) No 575/2013 to use the standardised methodology where it considers that the simplified standardised methodology is not adequate to capture interest rate risk arising from non-trading book activities of that credit institution.

Operational risk.

51.- (1) Credit institutions shall implement policies and procedures for the assessment and management of exposures to operational risk, including model risk and outsourcing risks, and to hedge the risk of low frequency events and serious consequences. Credit institutions shall clearly state what constitutes operational risk for the purposes of these policies and procedures.

(2) Credit institutions shall draw up plans for dealing with emergencies and continuing to operate in order to ensure, on an ongoing basis, the viability of the credit institution and to limit losses in the event of a serious disruption of its activity.

ICT and security risk.

52.- (1) Credit institutions, in accordance with the provisions of paragraph 7 of this Directive and section VI, shall have sound ICT and security risk management strategies, policies and procedures in place, and for this purpose they shall have effective and reliable ICT systems that cover all their important activities and ensure that they extract timely, accurate, consistent, complete and relevant information, in order to enable:

(a) the preparation of annual or periodic financial or non-financial statements for the financial profile and risk profile of the credit institution, for internal purposes, or external purposes as required by the regulatory framework;

(b) the effective management of decision making and supervision by the credit institution;

(c) effective information for the purposes of internal control of the credit institution and/or supervision; and

(d) to get an in-depth view on the effectiveness of risk management, compliance and internal control frameworks.

(2) Information systems, including those that store and process data in electronic form, shall be secured and supported by appropriate emergency settings.

(3) Credit institutions shall ensure that transaction records are kept in a systematic and secure manner, for a period of not less than ten (10) years and in a way that facilitates the production of audit logs and the restructuring of all transactions in chronological order, the verification of each of the recorded transaction in relation to the original invoices and the validation of any changes in the balances of the accounts in relation to the supporting documents that cover all the transactions leading to the aforementioned changes.

EBA/GL/2019/04 29.11.2019.

(4) Credit institutions shall comply with the provisions of the EBA Guidelines on ICT and security risk management, in such a way that takes account of the proportionality criteria specified in Part 2 of this Directive and by applying the general requirements of Section II of this Part.

Liquidity risk.

53.- (1) Credit institutions shall have robust strategies, policies, processes and systems for the identification, measurement, management and monitoring of liquidity risk over an appropriate set of time horizons, including intra-day, so as to ensure that adequate levels of liquidity buffers are maintained; those strategies, policies, processes and systems shall be tailored to business lines, currencies, branches and legal entities and shall include adequate allocation mechanisms of liquidity costs, benefits and risks.

(2) The strategies, policies, processes and systems referred to in subparagraph (1) shall be proportionate to the complexity, risk profile, scope of operation of the credit institutions and risk tolerance set by the management body and shall reflect the credit institution's importance in the Republic and in any other Member State in which it carries out business. Credit institutions shall communicate risk tolerance to all relevant business lines.

(3) Credit institutions shall develop methodologies for the identification, measurement, management and monitoring of funding positions; these methodologies shall include the current and projected

material cash-flows in and arising from assets, liabilities, off-balance sheet items, including contingent liabilities and the possible impact of reputational risk.

(4) Credit institutions shall distinguish between pledged and unencumbered assets that are available at all times, in particular during emergency situations; credit institutions shall take into account the legal entity in which assets reside, the country where assets are legally recorded either in a register or in an account and their eligibility and shall monitor how assets can be mobilised in a timely manner.

(5) Credit institutions shall have regard to existing legal, regulatory and operational limitations to potential transfers of liquidity and unencumbered assets amongst entities, both within and outside the European Economic Area.

(6) Credit institutions shall consider different liquidity risk mitigation tools, including a system of limits and liquidity buffers in order to be able to withstand a range of different stress events and an adequately diversified funding structure and access to funding sources; credit institutions shall ensure that these arrangements are reviewed regularly.

(7) Credit institutions shall consider alternative scenarios on liquidity positions and on risk mitigants and review the assumptions underlying decisions concerning the funding position at least annually; for these purposes, alternative scenarios shall address, in particular, off- balance sheet items and other contingent liabilities, including those of securitisation special purpose entities (SSPEs) or other special purpose entities, as referred to in the Regulation (EU) 575/2013, in relation to which the credit institution acts as sponsor or provides material liquidity support.

(8) Credit institutions shall consider the potential impact of credit institution-specific, market-wide and combined alternative scenarios; different time periods and varying degrees of stressed conditions shall be considered.

(9) Credit institutions shall adjust their strategies, internal policies and limits on liquidity risk and develop effective contingency plans, taking into account the outcome of the alternative scenarios referred to in subparagraph (8).

(10) (a) Credit institutions shall have in place liquidity recovery plans setting out adequate strategies and proper implementation measures in order to address possible liquidity shortfalls, including in relation to branches established in another Member State.

(b) Liquidity recovery plans shall be tested by credit institutions at least annually, updated on the basis of the outcome of the alternative scenarios set out in subparagraph (8), and be reported to and approved by the senior management so that internal policies and processes can be adjusted accordingly.

(c) Credit institutions shall take the necessary operational steps in advance to ensure that liquidity recovery plans can be implemented immediately by credit institutions. Such operational steps shall include holding collateral immediately available for funding by the competent authority. This includes holding collateral where necessary in the currency of another Member State, or currency of a third country to which the credit institution has exposures, and where operationally necessary within the territory of a host member state or of a third country to whose currency it is exposed.

Risk of excessive leverage.

54.- (1) Credit institutions shall have policies and processes in place for the identification, management and monitoring of the risk of excessive leverage; indicators for the risk of excessive leverage include the leverage ratio determined in accordance with Article 429 of Regulation (EU) No. 575/2013 and mismatches between assets and obligations.

(2) Credit institutions shall address the risk of excessive leverage in a precautionary manner by taking due account of potential increases in the risk of excessive leverage caused by reductions of the credit institution's own funds through expected or realised losses, depending on the applicable accounting rules; to that end, credit institutions shall be able to withstand a range of different stress events with respect to the risk of excessive leverage.

Section II – Internal control framework and mechanisms

Internal control framework.

55.- (1) Credit institutions shall develop and maintain a culture that encourages a positive attitude towards risk control and compliance within the credit institution and a robust and comprehensive internal control framework.

(2) Under this framework, credit institutions' business lines shall be responsible for managing the risks they incur in conducting their activities and shall have controls in place that aim to ensure compliance with internal and external requirements.

(3) As part of this framework, credit institutions shall have internal control functions with appropriate and sufficient authority, stature and access to the management body to fulfil their mission, and a risk management framework.

(4) The internal control framework of the credit institution concerned shall be adapted on an individual basis to the specificity of its business, its complexity, and the associated risks, taking into account the group context.

(5) The credit institutions concerned shall organise the exchange of the information necessary in a manner that ensures that each management body, business line and internal unit, including each internal control function, is able to carry out its corresponding duties. The credit institutions concerned shall ensure the necessary exchange of adequate information, for instance, between the business lines and the compliance function at the group level and between the heads of the internal control functions at the group level and the management body of the credit institution.

(6) Credit institutions shall implement appropriate procedures to ensure compliance with the obligations to prevent and combat money laundering. Credit institutions shall assess their exposure to the risk of being used for the purposes of money laundering and, where necessary, take mitigation measures to reduce these risks, as well as operational and reputational risks related to them. Credit institutions shall take steps to ensure that their staff are aware of these risks and their implications for the credit institution and the integrity of the financial system.

(7) The internal control framework shall cover the whole organisation, including the management body's responsibilities and tasks, and the activities of all business lines and internal units, including internal control functions, outsourced activities and distribution channels.

(8) The internal control framework of a credit institution shall ensure:

(a) effective and efficient operation;

(b) prudent conduct of business activities;

(c) adequate identification, measurement and mitigation of risks;

(d) the reliability of financial and non-financial information reported both internally and externally;

(e) sound administrative and accounting procedures; and

(f) compliance with laws, regulations, supervisory requirements and the credit institution's internal policies, processes, rules and decisions.

(9) Internal control functions shall be involved, having an advisory role, in establishing / designing new procedures.

Implementing an internal control framework.

56.- (1) The management body shall be responsible for establishing and monitoring the adequacy and effectiveness of the internal control framework, processes and mechanisms, and for overseeing all business lines and internal units, including internal control functions (such as risk management, compliance and internal audit functions). Credit institutions shall establish, maintain and regularly update adequate written internal control and ICT and security policies, mechanisms and procedures, which shall be approved by the management body.

(2) Credit institutions shall establish, maintain and update appropriate and documented policies, mechanisms and procedures of the internal control system at regular intervals, which shall be approved by the management body.

(3) A credit institution shall have a clear, transparent and documented decision-making process and a clear allocation of responsibilities and authority within its internal control framework, including its business lines, internal units and internal control functions.

(4) Credit institutions shall communicate those policies, mechanisms and procedures to all staff and every time material changes have been made.

(5) When implementing the internal control framework, credit institutions shall establish adequate segregation of duties – for instance, entrusting conflicting activities within the processing of transactions or when providing services to different persons, or entrusting supervisory and reporting responsibilities for conflicting activities to different persons – and establish information barriers, for instance, through the physical separation of certain departments.

(6) The internal control functions shall verify that the policies, mechanisms and procedures set out in the internal control framework are correctly implemented in their respective areas of competence.

(7) Credit institutions shall ensure that internal control systems include training in internal control mechanisms, in particular for employees in high-responsibility or high-risk positions.

(8) Internal control functions shall regularly submit to the management body written reports on major identified deficiencies. These reports shall include, for each new identified major deficiency, the relevant risks involved, an impact assessment, recommendations and corrective measures to be taken.

(9) The management body shall follow up on the findings of the internal control functions in a timely and effective manner and require adequate remedial actions. A formal follow-up procedure on findings and corrective measures taken shall be put in place.

Risk management framework.

57.- (1) As part of the overall internal control framework, credit institutions shall have a holistic credit institution-wide risk management framework extending across all its business lines and internal units, including internal control functions, recognising fully the economic substance of all its risk exposures it undertakes.

(a) The risk management framework shall enable the credit institution to make fully informed decisions on risk-taking.

(b) The risk management framework shall encompass on- and off-balance-sheet risks as well as actual risks and future risks that the credit institution may be exposed to.

(c) Risks shall be evaluated from the bottom up and from the top down, within and across business lines, using consistent terminology and compatible methodologies throughout the credit institution and at consolidated or sub-consolidated level.

(d) All relevant risks shall be encompassed in the risk management framework with appropriate consideration of both financial and non-financial risks, including credit, market, liquidity, concentration, operational, IT, reputational, legal, conduct, compliance and strategic risks.

(2) The credit institution's risk management framework shall include policies, procedures, risk limits and risk controls ensuring adequate, timely and continuous identification, measurement or assessment, monitoring, management, mitigation and reporting of the risks at the business line, credit institution and consolidated or sub-consolidated levels.

(3) Credit institutions shall ensure that each significant risk is associated with a policy, process or measure, as well as related controls to ensure that any such policy, process or other measure is implemented and operates as intended.

(4) An effective risk management framework requires as a minimum:

(a) assessing the risk capacity of the credit institution;

(b) establishing the risk appetite of the credit institution through the articulation in written form of a risk appetite statement;

(c) allocating the credit institution's risk appetite statement to business lines, business units, specific risk categories, concentrations, and other appropriate level in the form of risk limits;

(d) assessing the risk profile of the credit institution against its risk appetite;

(e) description of the roles and responsibilities of those overseeing the implementation and monitoring of the risk appetite framework.

(5) Credit institutions shall ensure that the risk appetite statement:

(a) is linked to the credit institutions' strategic, capital and financial plans, as well as compensation programs;

(b) establishes the level of risk the credit institution is prepared to accept in pursuit of its strategic objectives and business plan, taking into account the interests of its stakeholders as well as capital and other regulatory requirements;

(c) determines for each material activity the maximum level of risk that the credit institution is willing to operate within, based on its risk appetite, risk capacity, and risk profile;

(d) ensures that the strategy and risk limits of each business line and legal entity align with the credit institution-wide risk appetite statement as appropriate; and

(e) is forward looking and subject to scenario and stress testing to ensure that the credit institution understands what events might push the credit institution outside its risk appetite and its risk capacity.

(6) Credit institutions shall ensure that risk limits:

(a) are set at a level that constrains risk-taking within risk appetite based on an estimate of the impact on the interests of stakeholders, as well as capital and other regulatory requirements, in the event that a risk limit is breached and the likelihood that each material risk is realised;

(b) include material risk concentrations at the credit institution-wide, business line and business unit levels such as counterparty, industry, region, collateral type, currency and product;

(c) are monitored regularly.

(7) Credit institutions shall ensure that they have the necessary mechanisms to adapt the risk management framework to changing business and market conditions.

(8) Credit institutions shall ensure that breaches of risk limits occur escalate and are addressed with an appropriate follow-up procedure.

(9) The credit institution's risk management framework shall provide specific guidance on the implementation of its strategies. This guidance shall, where appropriate, establish and maintain internal limits consistent with the credit institution's risk appetite and commensurate with its sound operation, financial strength, capital base and strategic goals. A credit institution's risk profile shall be kept within these established limits. The risk management framework shall ensure that, whenever breaches of risk limits occur, there is a defined process to escalate and address them with an appropriate follow-up procedure.

(10) The risk management framework shall be subject to independent internal review to be performed by the internal audit function, and an external assessment, and shall be reassessed regularly against the credit institution's risk appetite, taking into account information from the risk management function and the risk committee.

(11) Factors that shall be considered include internal and external developments, including balance-sheet and revenue changes, any increase in the complexity of the credit institution's business, risk profile or operating structure; geographic expansion, mergers and acquisitions and the introduction of new products or business lines.

(12) (a) When identifying and measuring or assessing risks, a credit institution shall develop appropriate methodologies including both forward-looking and backward-looking tools. These methodologies shall allow for the aggregation of risk exposures across business lines and support the identification of risk concentrations.

(b) The tools foreseen in point (a) of this sub-paragraph, shall include the assessment of the actual risk profile against the credit institution's risk appetite, as well as the identification and assessment of potential and stressed risk exposures under a range of assumed adverse circumstances against the credit institution's risk capacity.

(c) The tools foreseen in point (a) of this sub-paragraph shall provide information on any adjustment to the risk profile that may be required. Credit institutions shall make appropriately conservative assumptions when building stressed scenarios.

(13) Credit institutions shall take into consideration that the results of quantitative assessment methodologies, including stress testing, are highly dependent on the limitations and assumptions of the models (including the severity and duration of the shock and the underlying risks). For example, models showing very high returns on economic capital may result from a weakness in the models, for instance the exclusion of some relevant risks, rather than a superior strategy or excellent execution of a strategy on the part of the credit institution.

(14) (a) The risk management framework shall include quantitative assessments which can be translated into risk limits applicable to business segments and units which in turn can be aggregated and disaggregated to allow the measurement of the risk profile in relation to the appetite of the credit institution for undertaking a risk and the capability of undertaking a risk;

(b) Subject to the provisions of sub-paragraph (1) of this paragraph, the determination of the level of risk taken shall not therefore be based only on quantitative information or the use of models; it shall also comprise a qualitative approach, including expert judgement and critical analysis. Relevant macroeconomic environmental trends and data shall be duly considered to identify their potential impact on exposures and portfolios.

(15) The ultimate responsibility for risk assessment lies solely and fully with the credit institution, which, accordingly, shall evaluate its risks critically and shall not rely exclusively on external assessments. The credit institution shall validate a purchased risk model and calibrate it to its own individual circumstances to ensure that the model accurately and comprehensively captures and analyses the risk.

(16) Credit institutions shall be fully aware of the limitations of models and metrics and use not only quantitative but also qualitative risk assessment tools, including expert judgement and critical analysis.

(17) (a) In addition to the credit institutions' own assessments, credit institutions may use external risk assessments, including external credit ratings or externally purchased risk models.

(b) Credit institutions shall be fully aware of the exact scope of such assessments and their limitations.

(18) (a) Regular and transparent reporting mechanisms shall be established so that the management body, its risk committee and all relevant units in a credit institution are provided with reports in a timely, accurate, concise, understandable and meaningful manner and can share relevant

information about the identification, measurement or assessment, monitoring and management of risks.

(b) The reporting framework shall be well defined and documented.

(19) Credit institutions shall make a written record on an individual and on a consolidated basis of:

(a) the major sources of risk identified;

(b) assessments of those risks including details of the stress tests and scenario analysis carried out;

(c) how they intend to deal with those risks; and

(d) the resulting financial resources estimated to be required as part of the internal capital adequacy process.

(20) (a) Effective communication and awareness regarding risks and the risk strategy is crucial for the whole risk management process, including the review and decision-making processes, and helps prevent decisions that may unknowingly increase risk.

(b) Effective risk reporting involves sound internal consideration and communication of risk strategy and relevant risk data (for instance, exposures and key risk indicators), both horizontally across the credit institution and up and down the management chain.

New products and significant changes.

EBA/GL/2015/18 15.07.2015.

58.- (1) Subject to EBA's Guidelines on product oversight and governance arrangements for retail banking products, the credit institution shall have in place a well-documented new product approval policy (NPAP), approved by the management body, that addresses the development of new markets, products and services, and significant changes to existing ones, as well as exceptional transactions.

(2) The new product approval policy shall encompass material changes to related processes, for instance new outsourcing arrangements and corresponding systems, for instance IT change processes.

(3) The new product approval policy shall ensure that approved products and changes are consistent with the risk strategy and risk appetite of the credit institution and the corresponding limits, or that necessary revisions are made.

(4) Material changes or exceptional transactions, referred to in sub-paragraph (1) as components of the new product approval policy, may include mergers and acquisitions, including the potential consequences of conducting insufficient due diligence that fails to identify post-merger risks and liabilities; setting up structures, for instance new subsidiaries or single purpose vehicles; new products; changes to systems or the risk management framework or procedures; and changes to the credit institution's organisation.

(5) The credit institution shall have specific procedures for assessing compliance with these policies, taking into account the input of the risk management function. This shall include a systematic prior assessment and documented opinion by the compliance function for new products or significant changes to existing products.

(6) The credit institution's new product approval policy, shall cover every consideration to be taken into account before deciding to enter new markets, deal in new products, launch a new service, or make significant changes to existing products or services.

(7) The new product approval policy shall also include the definitions of 'new product/market/business' and 'significant changes' to be used in the organisation and the internal functions to be involved in the decision-making process.

(8) The new product approval policy shall set out the main issues to be addressed before a decision is made. These shall include regulatory compliance; accounting; pricing models; the impact on risk profile, capital adequacy and profitability; the availability of adequate front, back and middle office resources; and the availability of adequate internal tools and expertise to understand and monitor the associated risks.

(9) Credit institutions shall identify and assess the risk of money laundering related to a new product or practice and take measures to mitigate the risk, in accordance with the Law on Preventing and Combating Money Laundering of 2007.

(10) The decision to launch a new activity shall clearly state the business unit and individuals responsible for it. A new activity shall not be undertaken until adequate resources to understand and manage the associated risks are available.

(11) The risk management function and the compliance function shall be involved in approving new products or significant changes to existing products, processes and systems. Their input shall include a full and objective assessment of risks arising from new activities under a variety of scenarios, of any potential shortcomings in the credit institution's risk, management and internal control frameworks, and of the ability of the credit institution to manage any new risks effectively.

(12) The risk management function shall also have a clear overview of the roll-out of new products, or significant changes to existing products, processes and systems) across different business lines and portfolios, and the power to require that changes to existing products go through the formal new product approval process.

Section III - Internal control functions

Internal control functions – General requirements.

59.- (1) The system of internal control functions shall include the following four individual functions: a risk management function, a compliance function, an internal audit function and an ICT and security function.

(2) The risk management, regulatory compliance and ICT and security functions shall be subject to review by the internal audit function.

(3) The obligations of the internal control functions shall also include ensuring the compliance of the credit institution with its requirements for the Prevention and Combating of Money Laundering Law of 2007.

(4) The operational tasks of the internal control functions may be outsourced, taking into account the proportionality criteria listed in Part 2 of this Directive, to the consolidating credit institution or another entity within or outside of the group with the consent of the management bodies of the credit institutions concerned.

(5) Even when internal control operational tasks are partially or fully outsourced, the head of the internal control function concerned, and the management body are still responsible for these activities and for maintaining an internal control function within the credit institution.

(6) The internal control functions shall have the right to contact any staff member on their own initiative and to gain access to any files or records or to any other form of information as necessary for the performance of their duties.

(7) Due to the close link between the activities of the internal control functions, the credit institution shall ensure that there is a clearly defined division and separation of responsibilities, in particular as regards liability for measuring risk, and identifying, verifying and assessing the adequacy of relevant internal control procedures and regulations.

(8) Each internal control shall have an obligation to notify other internal control functions of any findings that concerns them; these findings shall serve as a feedback mechanism for assessing the areas under responsibility of the control function for the relevant control policies and procedures.

(9) Subject to the provisions of the Prevention and Suppression of Money Laundering Activities Law of 2007, credit institutions shall be responsible for ensuring compliance of the credit institution in accordance with its requirements of the Prevention and Suppression of Money Laundering Activities Law of 2007, as well as the policies and procedures of the credit institution to a staff member responsible for the enforcement of the laws, regulations and administrative provisions necessary to comply with the Prevention and Suppression of Money Laundering Activities Law of 2007 (for instance chief compliance officer). Credit institutions may establish a separate compliance function for preventing and combating money laundering and terrorist financing, as an independent control function. The person responsible for the function of preventing and combating money laundering shall, where required, be able to report directly to the management body.

(10) Credit institutions shall, wherever possible and without compromising the competence and expertise in the area of operations of the internal control functions, periodically rotate the staff of each internal control function or transfer staff from one internal control function to another operation of the credit institution, in order to ensure that the sound judgment of the employees of an internal control function is not called into question due to the possible loss of objectivity from the continuous execution of similar tasks or routine tasks.

(11) The rotation of staff roles and positions within an internal control function and the transfer of staff to and from an internal control function, shall be governed by, and carried out in accordance with, a sound and recorded policy. This policy must be designed in such a way so as to avoid conflicts of interest and to ensure that:

(a) adequate time has elapsed, suitable for the size and complexity of the credit institution, before the assignment to staff of any oversight responsibilities relating to the internal control function in which such member of staff used to work, before being transferred to his new position;

(b) the process of staff reassignments has minimum disruption to the operations of the internal control function.

(12) The management body shall ensure that appropriate controls are in place for each significant business process and policy and for associated risks and obligations.

(13) The internal control functions shall ensure that the communication with chief executives, the management body and the relevant committees is sufficiently documented.

Manual of the internal control function.

60.- (1) The purpose, standing and authority of an internal control function shall be governed by a manual which shall be periodically reviewed by the head of the internal control function and approved by the management body.

(2) The manual shall define, as a minimum, the following:

(a) the internal control function's status within the credit institution, its authority, its purpose and scope, its key features and responsibilities, its communication lines and its relations with other internal control functions in a manner that promotes its effectiveness;

(b) measures to ensure its independence;

(c) its right to initiate communication with any member of staff, to obtain full and unconditional access to all records and files of the credit institution as well as any other information necessary to carry out its responsibilities;

(d) its right to freely express and report its findings to the management body and its relevant committees without the presence of executive members of the management body;

(e) the terms and conditions according to which the internal control function can be called upon to provide consulting or advisory services or to carry out other special tasks;

(f) its role in the approval of new products and services, the development of new markets, and significant changes to existing ones;

(g) the responsibility and accountability of the head of the internal control function;

(h) a requirement to comply with professional standards.

Heads of the internal control functions.

61.- (1) The heads of the internal control functions shall be appointed at an appropriate hierarchical level that provides the head of the control function with the appropriate authority and stature needed to fulfil his or her responsibilities.

(2) Notwithstanding the overall responsibility of the management body, heads of internal control functions shall be independent of the business lines or units they control. To this end, the heads of the risk management, compliance, internal audit and ICT and security functions shall report and be directly accountable to the management body, and their performance shall be reviewed by the management body.

(3) Where necessary, the heads of internal control functions shall be able to have access and report directly to the management body and/or its committees, in order to raise concerns and warn where appropriate, when the credit institution is affected or may be affected by specific developments and/or in the event of specific risk developments affecting or likely to affect the credit institution, without prejudice to the responsibilities of the management body in accordance with the harmonising provisions of Directive 2013/36/EU and Regulation (EU) no. 575/2013. This possibility shall not prevent the heads of internal control functions from reporting within the regular reporting lines as well.

(4) Heads of the internal control functions shall be responsible for:

(a) ensuring the objectivity and independence of the control function;

(b) acquiring human resources with sufficient qualifications and skills to ensure the competence of the control function to carry out its tasks and responsibilities;

(c) continually assessing and monitoring the skills necessary to carry out the function's duties to the required level;

(d) ensuring the appropriate ongoing training of the control function staff in order to carry out the increasing diversity of tasks that need to be undertaken as a result of the introduction of new products and processes within the credit institution, changes to regulations or professional standards and other developments in the financial sector;

(e) promptly informing the heads of other internal control functions for any findings relating to them;

(f) submitting reports to the management body and relevant committees and attending their meetings to present the said reports and provide additional information and/or clarification or assistance on managing the issues raised;

(g) on the selection as well as the fitness of the persons in charge of the respective internal control functions of subsidiaries in Cyprus and abroad as well as those appointed overseas in branches;

(h) expressing an opinion, in case where the credit institution is a parent undertaking of a group, on the selection as well as the fitness of the persons in charge of the respective internal control functions of subsidiaries in Cyprus and abroad as well as those appointed overseas in branches;

(i) updating the competent authority of any significant findings on, or developments that came to his or her attention that have material impact on, the credit institution's risk profile and of any significant changes in the structure and functions of the internal control function concerned;

(j) holding meetings with the competent authority at any other interval the competent authority may require to discuss the scope and coverage of the work of the internal control function, its risk analysis, findings and recommendations.

(5) The credit institution shall have documented processes in place regarding the appointment and removal of a head of an internal control function.

(6) In any case, the heads of internal control functions shall not be removed without the prior approval of the management body.

(7) Subject to the provisions of the Directive on the Assessment of Suitability of the Members of the Management Body and Key Function Holders of Authorised Credit institutions of 2020, credit institutions shall promptly inform the competent authority about the approval and the main reasons for the removal of a head of an internal control function.

(8) The heads of internal control functions shall receive any report or information or communication sent by the competent supervisory authorities to the credit institution which contains findings and comments regarding their responsibilities as defined by this Directive.

Independence of operations of internal control functions.

62.- Internal control functions shall be deemed to be independent if the following conditions are met:

(a) their staff do not perform any operational tasks that fall within the scope of the activities the internal control functions are intended to monitor and control;

(b) they are organisationally separate from the activities they are assigned to monitor and control;

(c) notwithstanding the overall responsibility of members of the management body for the credit institution, the head of an internal control function shall not be subordinate to a person who has responsibility for managing the activities the internal control function monitors and controls; and

(d) the remuneration of the internal control functions' staff shall not be linked to the performance of the activities the internal control function monitors and controls, and not otherwise likely to compromise their objectivity.

Combination of operations of internal control functions.

63.- (1) Taking into account the proportionality criteria set out in Part 2, the risk management function, the compliance function and the ICT and security functions may be combined, provided that the prior approval of a combination of the competent authority has been obtained. In any case, any combination shall not contain more than two of these functions.

(2) The internal audit function shall not be combined with another internal control function.

Resources of internal control functions.

64.- (1) Internal control functions shall have sufficient resources. They shall have an adequate number of qualified staff, both at parent level and at subsidiary level. Staff shall remain qualified on an ongoing basis and shall receive training as necessary.

(2) Internal control functions shall have appropriate IT systems and support at their disposal, with access to the internal and external information necessary to meet their responsibilities. They shall have access to all necessary information regarding all business lines and relevant risk-bearing subsidiaries, in particular those that can potentially generate material risks for the credit institution.

Section IV - Risk management function

Risk management function – General requirements.

65.- (1) Credit institutions shall establish a risk management function, covering the whole credit institution. Taking into account the proportionality criteria listed in Part 2, the risk management function shall be independent from operational functions and shall have sufficient authority, stature and resources, in order to be able to implement risk policies and the risk management framework as set out in paragraph 57 of this Directive.

The risk management function shall report to the management body through the risk committee.

(2) The risk management function shall have, where necessary, and independently of senior management, direct access to the management body and its committees, including in particular the risk committee, raise concerns and warn the management body, when appropriate, in case of specific risk developments affecting or likely to affect the credit institution, regardless of the responsibilities of the management body in the exercise of supervisory and / or administrative of powers, pursuant to the harmonising provisions of Directive 2013/36/EU and Regulation (EU) No 575/2013.

(3) The risk management function shall have access to all business lines and other internal units that have the potential to generate risk, as well as to relevant subsidiaries and affiliates.

(4) Staff within the risk management function shall possess sufficient knowledge, skills and experience in relation to risk management techniques and procedures.

(5) The risk management function shall be independent of the business lines and units whose risks it controls but shall not be isolated, namely, it shall not be prevented from interacting with such lines and units.

(6) Interaction between the operational function and the risk management function, shall help to achieve the objective of all the credit institution's staff bearing responsibility for managing risk.

(7) The risk management function:

(a) shall be a central organisational feature of the credit institution, structured so that it can implement risk policies and control the risk management framework;

(b) shall play a key role in ensuring that the credit institution has effective risk management processes in place;

(c) shall be actively involved in all material risk management decisions.

(8) Significant credit institutions may consider establishing dedicated risk management functions for each material business line. However, there shall be a central risk management function, including a group risk management function in the consolidating credit institution, to deliver a credit institution- and group-wide holistic view on all risks and to ensure that the risk strategy is complied with.

(9) The risk management function shall provide relevant independent information, analyses and expert judgement on risk exposures, and advice on proposals and risk decisions made by business lines or internal units and shall inform the management body as to whether they are consistent with the credit institution's risk appetite and strategy.

(10) The risk management function may recommend improvements to the risk management framework and corrective measures to remedy breaches of risk policies, procedures and limits.

The role of the risk management function in risk strategy and in risk-related decisions.

66.- (1) The risk management function, shall be actively involved at an early stage in elaborating a credit institution's risk strategy and in ensuring that the credit institution has effective risk management processes in place.

(2) The risk management function shall be actively involved in the detailed elaboration and development of the credit strategy of the credit institution as well as in all important risk management decisions and shall be able to give a complete picture of the whole range of risks faced by the credit institution.

(3) The risk management function shall provide the management body with any relevant risk-related information in order to facilitate the determination of the credit institution's level of risk appetite.

(4) The risk management function shall evaluate the completeness and viability of the risk strategy and risk appetite. It shall ensure that the risk appetite is properly translated into specific risk limits.

(5) The risk management function shall evaluate the risk strategies of the business units, including the objectives proposed by the business units, while it shall also be involved in the process before the management body makes a decision regarding the risk strategies. Objectives shall be reasonable, consistent with the credit institutions' risk strategy, and include reliable credit ratings and return on equity ratios.

(6) The risk management function shall be adequately involved in any changes to the credit institution's strategy, risk appetite framework and risk limits.

(7) The risk management function shall play a key role in ensuring a decision on its recommendation is made at the relevant level, complied with by the relevant business units and appropriately reported to the management body, risk committee and business or support unit.

(8) The risk management function's involvement in decision-making processes shall ensure that risk considerations are taken into account appropriately. However, accountability for the decisions taken shall remain with the business and internal units, and ultimately the management body.

The role of the risk management function in material changes.

67.- (1) In accordance with the provisions of paragraph 58 of this Directive, before any decisions on material changes or exceptional transactions are taken, the risk management function shall be involved in the evaluation of the impact of such changes and exceptional transactions on the credit institution's and group's overall risk, and shall report its findings directly to the management body before a decision is taken.

(2) The risk management function shall evaluate how risks identified could affect the credit institution's or group's ability to manage its risk profile, its liquidity and its sound capital base under normal and adverse circumstances.

The role of the risk management function in identifying, measuring, assessing, managing, mitigating, monitoring and reporting on risks.

68.- (1) The risk management function, shall ensure that all risks are identified, assessed, measured, monitored, managed and properly reported on by the relevant units in the credit institution.

(2) The risk management function shall ensure that identification and assessment are not based only on quantitative information or model outputs and take into account also qualitative approaches.

(3) The risk management function shall keep the management body informed of the assumptions used in and potential shortcomings of the risk models and analysis.

(4) The risk management function shall be actively involved at the primary stage in the evaluation of the impact of significant changes in the structure of the credit institution and of unusual transactions in the total risk of the credit institution and the group, before decisions on material changes or exceptional transactions are taken.

(5) The risk management function shall ensure that transactions with related parties are reviewed and that the risks they pose for the credit institution are identified and adequately assessed.

(6) The risk management function shall ensure that all identified risks are effectively monitored by the business units.

(7) The risk management function shall regularly monitor the actual risk profile of the credit institution and scrutinise it against the credit institution's strategic goals and risk appetite to enable decision-making by the management body and challenge by the management body.

(8) The risk management function shall analyse trends and recognise new or emerging risks and risk increases arising from changing circumstances and conditions. It shall also regularly review actual risk outcomes against previous estimates, for instance, back testing, to assess and improve the accuracy and effectiveness of the risk management process.

(9) The risk management function shall evaluate possible ways to mitigate risks. Reporting to the management body shall include proposed appropriate risk-mitigating actions.

The role of the risk management function in handling unapproved exposures.

69.- (1) The risk management function shall independently assess breaches of risk appetite or limits, including ascertaining the cause and undertaking a legal and economic analysis of the actual cost of closing, reducing, or hedging the exposure against the potential cost of keeping it.

(2) In relation to the assessment foreseen by sub-paragraph (1) of this paragraph, the risk management function shall inform the business units concerned and the management body and recommend possible remedies. When the breach is material, the risk management function shall report directly to the management body, without prejudice to the obligation of the risk management function to report to other internal functions and committees.

(3) The risk management function shall play a key role in ensuring a decision on its recommendation is made at the relevant level, complied with by the relevant business units and appropriately reported to the management body and, where established, the risk committee.

Head of the risk management function.

70.- (1) Subject to the provisions of paragraph 60 of this Directive, the head of the risk management function of the credit institution, and of a parent credit institution regarding the consolidated situation, shall be responsible for providing a comprehensive and understandable information on risks and advising the management body, enabling it to understand the credit institution's overall risk profile.

(2) The head of the risk management function shall have sufficient expertise, independence and seniority to challenge decisions that affect a credit institution's exposure to risks.

(3) Subject to sub-paragraph (4) of this paragraph, credit institutions shall appoint an independent head of the risk management function, who has no responsibilities for other functions of the credit institution and reports directly to the management body.

(4) Where it is not proportionate to appoint a person who is dedicated only to the role of head of the risk management function, taking into account the principle of proportionality as set out in Part 2 of this Directive, this function can be combined with the head of the compliance function or can be performed by another senior person, provided there is no conflict of interest between the functions combined. In any case, this person shall have sufficient authority, stature and independence.

(5) The head of the risk management function shall be able to challenge decisions taken by the credit institution's management and its management body, and the grounds for objections shall be formally documented.

(6) If a credit institution wishes to grant the head of the risk management function the right to veto decisions, for instance a credit or investment decision or the setting of a limit, made at levels below the management body, it shall specify the scope of such a veto right, the escalation or appeal procedures, and how the management body will be involved.

(7) Credit institutions shall establish strengthened processes for the approval of decisions on which the head of the risk management function has expressed a negative view.

(8) The management body shall be able to communicate directly with the head of the risk management function on key risk issues, including developments that may be inconsistent with the credit institution's risk appetite and strategy.

Reporting requirements of the risk management function.

71.- (1) Subject to the provisions of this Section, the head of the risk management function shall submit a report to the risk committee on a quarterly basis which will also be copied to the chief executive; the report should cover, as a minimum, the following:

(a) internal assessment and measurement of the risks faced by the credit institution;

(b) results and assumptions of stress tests or scenario analyses;

(c) calculation of capital requirements and capital adequacy ratio; and

(d) information about the external environment to identify market conditions and trends that may have a bearing on the credit institution's current and future risk profile.

(2) The head of the risk management function shall submit an annual report to the management body within two months from the end of each year, through the risk committee, which will also be copied to the chief executive, with the following minimum information:

(a) review of the main financial developments during the year which had a significant influence on the credit institution's operations and risk profile;

(b) description of the risk management framework, including the organisation and operation of the risk management function, and of the risk management process in place;

(c) assumptions and results of stress tests and scenario analyses carried out during the year under review;

(d) detailed information on the risk profile of the institution and the capital allocation process;

(e) summary of the results of the risk and control self-assessment exercise conducted during the year under review together with recommendations for minimising any increased operational risks identified;

(f) information on operational losses incurred during the year under review;

(g) information on key risk indicators and key performance indicators on nonperforming loans monitored by the credit institution;

(h) calculation of the credit institution's capital requirements and capital adequacy ratio;

(i) recommendations and specific measures to be taken for addressing any weaknesses identified in the risk management framework of the credit institution; and

(j) a comprehensive gap analysis section whereby the risk management function will comment on the recommendations made in its report of the previous year including an assessment of the progress achieved and the current status.

Section V - Compliance function

Compliance function – General requirements.

72.- (1) Credit institutions shall establish a permanent and effective compliance function to manage compliance risk and shall appoint a person to be responsible as head for this function across the entire credit institution.

(2) Where it is not proportionate to appoint a person who is dedicated only to the role of head of compliance, taking into account the principle of proportionality as set out in Part 2 of this Directive, this function can be combined with the head of the head of the risk management function or r can be performed by another senior officer, for instance head of legal, provided there is no conflict of interest between the functions combined.

(3) The compliance function, including the head of compliance, shall be independent of the business lines and internal units it controls and have sufficient authority, stature and resources. The compliance function shall account to the management body through the audit committee and shall inform senior management of its findings, in accordance with the provisions of this Directive.

(4) Taking into account the proportionality criteria set out in Part 2, the compliance function may be assisted by the risk management function or combined with the risk management function or other appropriate functions, for instance the legal division or human resources.

(5) Staff within the compliance function shall possess sufficient knowledge, skills and experience in relation to compliance and relevant procedures, and shall have access to guidance, support and regular training to assist them in fulfilling their obligations.

(6) The management body shall oversee the implementation of a well-documented compliance policy, which shall be communicated to all staff.

(7) Credit institutions shall set up a process to regularly assess changes in the law and regulations applicable to its activities.

(8) Credit institutions shall design, develop and implement an integrated compliance framework based on regulatory policy and supported by regulatory planning, procedures and safeguards.

(9) Credit institutions shall ensure that their regulatory compliance framework includes at least a regulatory compliance policy that defines the business and legal environment applicable to the institution and sets out the objectives, principles and allocation of regulatory responsibilities. In the case of a group, regulatory compliance policy indicates how compliance responsibilities are allocated and handled at group and credit institution level.

(10) Credit institutions shall ensure that their compliance identification process covers the following areas of compliance:

(a) the institution’s code of business conduct and corporate values;

(b) prudential laws and regulations;

(c) arrangements for the prevention of money laundering and terrorist financing;

(d) arrangements for the provision of investment services and activities;

(e) tax laws that are relevant to the structuring of banking products or customer advice;

(f) other regulations applicable to institutions such as regulations on consumer rights, data protection and competition;

(g) accounting and auditing requirements;

(h) business standards and best practices such as on –

(i) market conduct;

(ii) managing conflicts of interest;

(iii) treating customers fairly and ensuring the suitability of advice to customers;

(iv) information technology and electronic banking.

(11) Credit institutions shall ensure that that their compliance monitoring processes and procedures are regularly submitted to the staff appointed as regulatory compliance officers in large business units, branches and subsidiaries in the Republic and abroad to carry out regulatory compliance tasks, in order to assist such staff in carrying out their compliance duties.

(12) The regulatory compliance framework should include methods and procedures for establishing and maintaining an up-to-date register of legal, internal, regulatory, and operational requirements. There should be mechanisms and procedures for proper and effective access of staff to it and

appropriate staff alert mechanisms for changes to the framework and the relevant register, so that each staff member is kept informed of the requirements that affect and affect his tasks and duties.

(13) Credit institutions shall establish a formal and well-documented mechanism for providing instructions and assigning responsibilities for:

(i) assessing the causes of non-compliance;

(ii) initiating, requesting, implementing and monitoring the effectiveness of corrective measures; and

(iii) documenting the whole procedure and the outcome of the procedure.

(14) The compliance function should advise the management body on measures to be taken to ensure compliance with applicable laws, rules, regulations and standards, and should assess the possible impact of any changes in the legal or regulatory environment on the institution's activities and compliance framework.

(15) The compliance function should ensure that compliance monitoring is carried out through a structured and well-defined compliance monitoring programme and that the compliance policy is observed.

(16) The compliance function should report to the management body and communicate as appropriate with the RMF on the institution's compliance risk and its management.

(17) The compliance function and the risk management function should cooperate and exchange information as appropriate to perform their respective tasks. The findings of the compliance function should be taken into account by the management body and the risk management function in decision-making processes.

(18) In line with paragraph 58 of this Directive, the compliance function should also verify, in close cooperation with the risk management function and the legal unit, that new products and new procedures comply with the current legal framework and, where appropriate, with any known forthcoming changes to legislation, regulations and supervisory requirements.

(19) Credit institutions should take appropriate action against internal or external fraudulent behaviour which could facilitate fraud, or activities related to money laundering and terrorist financing and other cases of financial crime and disciplinary misconduct, such as for instance breach of internal procedures or breaches of limits.

(20) Credit institutions should ensure that their subsidiaries and branches take steps to ensure that their operations are compliant with local laws and regulations. If local laws and regulations hamper the application of stricter procedures and compliance systems implemented by the group, especially if they prevent the disclosure and exchange of necessary information between entities within the group, subsidiaries and branches should inform the compliance officer or the head of compliance of the consolidating institution.

(21) Credit institutions shall develop an integrated and institution-wide compliance culture-

(a) that is based on –

(i) a full understanding of regulations, national and international standards and best practices applicable to them; and

(ii) the compliance risks they face and how these risks are managed; and

(b) that is in line with their code of business conduct and corporate values; credit institutions should develop their compliance culture through policies, examples, communication and training of staff regarding their responsibilities for compliance.

(22) Credit institutions shall ensure that the compliance culture is appropriately disseminated at all hierarchical levels, with the objective of raising awareness and ensuring that each member of staff–

(a) understands the regulations, standards and best practices associated with the discharge of its operational or supervisory duties;

(b) understands associated compliance risks and the need and responsibility for managing these risks; and

(c) understands the importance of internal control functions in managing compliance risks and facilitates their tasks.

(23) The compliance function shall establish, implement and maintain appropriate mechanisms and activities –

(a) to promote and sustain a corporate culture of compliance and integrity within the institution;

(b) to assist senior management to design, develop and implement an appropriate and effective compliance framework for:

(i) the prompt and on-going compliance of the institution and its subsidiary companies in Cyprus and abroad and its foreign branches with their legal, regulatory and business obligations;

(ii) the effective management of risks of non-compliance with these obligations.

(24) Compliance activities shall be set out in a compliance programme prepared and monitored by the head of the compliance function that ensures that all relevant areas of the institution, its subsidiaries in Cyprus and abroad and foreign branches are appropriately covered, taking into account their susceptibility to compliance risk; the compliance activities shall include at least the following:

(a) identifying, on an on going basis, with the assistance of the institution's legal services unit and other competent units of the institution, of legal, regulatory and business requirements which govern and/or affect the operations of the institution;

(b) communicating to business units, branches and subsidiaries the legal, regulatory and business requirements applicable to them in –

(i) identifying the compliance obligations emanating from these requirements;

(ii) measuring and assessing the impact of these obligations on the institution's processes, procedures and operations;

(iii) assessing the appropriateness of the institution's compliance policies and procedures, following up deficiencies and, where necessary, formulating proposals for amendments;

(c) identifying and documenting the compliance risks associated with the institution's business activities, on a pro-active basis

(d) developing appropriate practices and methodologies to measure compliance risk such as risk indicators, with the assistance, if deemed necessary, of experts from the risk management function and using such measurements to enhance compliance risk assessment; the compliance function should ensure that these methodologies allow the aggregation or filtering of data that may be indicative of potential compliance problems;

(e) ensuring the use of appropriate tools and methodologies for monitoring activities which, inter alia, include:

(f) ensuring the use of appropriate tools and methodologies for monitoring activities which, inter alia, include:

(i) the assessment of periodic reports submitted by compliance officers

(ii) the use of aggregated risk measurements such as risk indicators;

(iii) the use of reports warranting management attention, documenting material deviations between actual occurrences and expectations (an exceptions report) or situations requiring resolution (an issues log);

(iv) targeted trade surveillance, observation of procedures, desk reviews and/or interviewing relevant staff;

(v) the verification of how compliance policies and procedures are implemented in practice through on-site inspections; and

(vi) the investigation of possible breaches of the compliance policy and regulatory framework with the assistance, if deemed necessary, of experts from within the institution such as experts from the internal audit function or legal services unit;

(g) ensuring there is an internal alert procedure in place to facilitate the confidential reporting by employees of concerns, shortcomings, or potential violations in respect of institutions policies, legal, regulatory or business obligations, or ethical considerations;

(h) overseeing the complaints process and utilising customer complaints as a source of relevant information in the context of its general monitoring responsibilities;

(i) periodically reassessing and reviewing the scope of compliance reviews to be performed;

(j) cooperating and exchanging information with other internal control and risk management functions on compliance matters;

(k) reporting promptly to senior management and the management body on material compliance failures and weaknesses in policy and internal control procedures as well as breaches of the regulatory framework revealed from its monitoring activity, on-site reviews and investigations;

(l) organising regular training and educational programs for management and staff on compliance and regulatory matters;

(m) advising and responding to queries on compliance issues from staff;

(n) issuing written instructions and circulars to staff, business units and the competent departments of the institution and the group for the prompt adjustment of internal procedures and regulations to changes in regulatory framework;

(o) verifying that new products and procedures comply with the current legal environment and business standards and any known changes to legislation, regulations, supervisory requirements and business standards.

Reporting requirements of the compliance function.

73.- (1) The head of the compliance function shall submit a report, to the audit committee on a quarterly basis which will also be copied to chief executive; the report should cover, as a minimum, the following:

(a) information on key compliance risk indicators monitored by the credit institution;

(b) material compliance issues and the status of any associated investigations or other actions being taken;

(c) up-to-date information on the institution's business and regulatory environment to identify developments that may have a bearing on the institution's current and future compliance obligations;

(d) brief details on the above for each subsidiary in Cyprus and abroad and foreign branches;

(e) material fines or other disciplinary actions taken by supervisory authorities in respect of the institution or any employee.

(2) The head of the compliance function shall submit an annual report to the management body within two months from the end of each year, through the audit committee, which will also be copied to the chief executive, with the following minimum information:

(a) description of the compliance framework, including the organisation and operation of the compliance function, and of the compliance management process in place;

(b) the compliance programme for the year under review;

(c) the compliance activities carried out during the year;

(d) summary, coupled with comprehensive comments, of the major findings and weaknesses identified from the review of the compliance policy and procedures carried out during the year under review and recommendations for corrective actions;

(e) an up-to-date summary of the progress achieved in the implementation and the effectiveness of the corrective actions taken in addressing any compliance related weaknesses and findings identified in the various reports of internal control functions, external auditors and advisors as well as those of the supervisory authorities;

(f) assessment of key compliance risks faced by the institution based on risk indicators and the steps being taken to address them;

(g) an up-to-date summary of changes and developments in legal, regulatory and business requirements occurred over the year and expected to occur in the near future and the measures taken and to be taken to ensure compliance with the changed requirements;

(h) details on the above for each subsidiary in Cyprus and abroad and foreign branches;

(i) an up-to-date summary of material correspondence with competent authorities;

(j) the compliance program and action plan of the compliance function for the following year.

(3) In relation to the monitoring procedures of cases of non-compliance with the Law and this Directive, the competent authority:

(a) for cases of non-compliance, it shall be notified within one (1) month from the date of their detection, together with information regarding the nature of the breach, the procedure that was followed or is being followed and the persons involved in the process of handling and resolving such cases, and

(b) for the corrective measures taken to address these cases, it shall be notified within two (2) months from the date of detection of a case of non-compliance.

Role of the compliance function in the prevention of money laundering activities.

74.- The compliance function shall ensure the institution's compliance with the Prevention and Suppression of Money Laundering Activities Law of 2007 and of the Directives of the Central Bank for the prevention of money laundering and terrorist financing issued in accordance with article 59(4) of the said Law, as well as of the relevant circulars of the Central Bank. the head of the compliance function or another member of the compliance function holding a managerial position should be appointed to the post of Head of Compliance under section 69 of the said Law, subject to the requirements of the said Law.

Section VI - ICT and security risk management function

ICT and security risk management function – General requirements.

75.- (1) Subject to the provisions of sub-paragraph (3) of paragraph 5, credit institutions should set up an ICT and security risk management function, covering the entire institution. Credit institutions should ensure the independence and objectivity of this control function, properly separating it from the processes of ICT functions. This control function should be directly accountable to the management body and be responsible for monitoring and controlling compliance with the ICT and security function, including the information security policy, as defined in paragraph 52. It should ensure the identification, measurement, assessment, management, monitoring and reporting ICT and safety risks. The ICT and security risk management function shall report to the management body through the risk committee.

(2) Subject to sub-paragraph (16) of paragraph 7 of this Directive, credit institutions shall ensure that all members of staff, including key function holders, receive appropriate ICT and security risk management training, including information security, on an annual basis or more frequently, if required.

Reporting requirements of the ICT and security risk management function.

76.- The head of the ICT and security risk management function, submits an annual report to the management body, through the risk committee, a copy of which is notified to the managing director. The reporting period of the report shall concern the respective calendar year unless the period is differentiated in consultation with the competent authority. The annual report is submitted to the management body within one month from the end of the reporting period. The report shall at least cover the following:

(a) a summary of the most significant ICT and security risks faced by the credit institution during the year under review;

(b) a list of all significant information security incidents that occurred during the year under review and the corrective action taken to prevent a recurrence of similar incidents;

(c) a summary of actions during the reporting year under review concerning the provision of training to staff on ICT and security risks;

(d) any significant actions taken during the year under review to improve weaknesses in the information security environment; and

(e) any outstanding issues that endanger the information security of the credit institution.

Section VII – Internal audit function

Internal audit function – General requirements.

77.- (1) Credit institutions shall set up an independent and effective internal audit function, taking into account the proportionality criteria set out in Part 2, and shall appoint a person to be responsible for this function across the entire credit institution.

(2) The internal audit function shall be independent and have sufficient authority, stature and resources. The internal audit function shall report to the management body through the audit committee and inform senior management of its findings, in accordance with the provisions of this Directive.

(3) The credit institution shall ensure that the qualification of the IAF's staff members and the IAF's resources, in particular its auditing tools and risk analysis methods, are adequate for the credit institution's size and locations, and the nature, scale and complexity of the risks associated with the credit institution's business model, activities, risk culture and risk appetite.

(4) The internal audit function shall be independent of the audited activities. Therefore, the internal audit function shall not be combined with other functions.

(5) The internal audit function, shall, following a risk-based approach, independently review and provide objective assurance of the compliance of all activities and units of a credit institution, including outsourced activities, with the credit institution's policies and procedures and with external requirements. Each entity within the group shall fall within the scope of the internal audit function.

(6) The internal audit function shall not be involved in designing, selecting, establishing and implementing specific internal control policies, mechanisms and procedures, and risk limits.

The internal audit function may provide information on matters relating to the risks and internal audits upon request of senior management, provided that the independence of the mission is not called into question.

(7) The internal audit function shall assess whether the credit institution's internal control framework as set out in paragraph 55 of this Directive.

In particular, the internal audit function shall perform audit assignments in accordance with paragraph 78 on its own initiative in all areas and functions of the credit institution, in accordance with the audit plan prepared by the head of the internal audit function and approved by the management body, to provide independent assurance to the management body in relation to issues such as:

(a) the appropriateness of the credit institution's governance framework;

(b) whether existing policies and procedures remain adequate and comply with legal and regulatory requirements and with the risk appetite and strategy of the credit institution;

(c) the compliance of the procedures with the applicable laws and regulations and with decisions of the management body;

(d) whether the procedures are correctly and effectively implemented, for instance, compliance of transactions or the level of risk effectively incurred;

(e) the adequacy, quality and effectiveness of the controls performed, and the reporting done by the defence business units and the risk management and compliance functions.;

(f) the accuracy of the reports submitted to the competent authority;

(g) the overall means by which the institution manages and mitigates the risks of safeguarding its assets, and seeks to prevent fraud, embezzlement, or misappropriation of such assets;

(h) the planning and operational effectiveness of the individual audits and of the operations of the internal control functions of the credit institution in relation to the aforementioned issues, as well as of all those audits;

(i) other matters that may be requested by the management body, senior management or the competent authority; and

(j) other issues that the internal audit function requires review in order to fulfil its mission.

(8) The internal audit function, shall verify, in particular, the integrity of the processes ensuring the reliability of the credit institution's methods and techniques, and the assumptions and sources of information used in its internal models, for instance, risk modelling and accounting measurements. It shall also evaluate the quality and use of qualitative risk identification and assessment tools and the risk mitigation measures taken.

(9) The internal audit function shall have unfettered credit institution-wide access to all the records, documents, information and buildings of the credit institution. This shall include access to management information systems and minutes of all committees and decision-making bodies.

(10) The internal audit function shall adhere to national and international professional standards. An example of the professional standards referred to here is the standards established by the Institute of Internal Auditors.

(11) The staff of the internal audit function must –

(a) act with integrity, carry out his or her duties in an honest and professional manner and inform the head of the internal audit function, if his or her ability to carry out an audit mission is called into question;

(b) exercise due diligence in the protection of information obtained in the performance of his or her duties;

(c) ensure that his professional views are not influenced by any personal or professional interests.

(12) Internal audit work shall be performed in accordance with an audit plan and a detailed audit programme following a risk-based approach.

(13) An internal audit plan shall be drawn up at least once a year on the basis of the annual internal audit control objectives. The internal audit plan shall be approved by the management body.

(14) All audit recommendations shall be subject to a formal follow-up procedure by the appropriate levels of management to ensure and report on their effective and timely implementation and relevant reports shall be submitted.

Audit assignments.

78.- (1) The internal audit function shall carry out such assignments as are needed to fulfil its responsibilities to provide assurance in accordance with paragraph 76, through routine audits and special audits, both announced and unannounced.

(2) The following audit activities shall be included, as a minimum, in its scope of internal audit assignments:

(a) assessment of the appropriateness and adequacy of the organisational structure and human resource management and the extent to which the credit institution has established appropriate corporate governance policies and procedures;

(b) assessment of the extent to which the credit institution's collective bodies as well as its operational units and internal control units effectively utilise the means and resources made available to them, follow the directions and procedures which have been officially set, whether due attention is paid towards ensuring the completeness and accuracy of information and whether they arrange to integrate in all procedures and transactions carried out, appropriate risk preventive and control mechanisms;

(c) assessment of the effectiveness, adequacy and adherence to the risk management and compliance procedures;

(d) assessment of the integrity of information technology systems including the risk management and accounting information systems as well as the accuracy, reliability and completeness of the information data used or produced;

(e) assessment of systems and procedures which govern the production of reliable, complete and up-to-date financial, management and regulatory information;

(f) assessment of the credit institution's information security for information of any kind, residing on any media including information in printed format;

(g) assessment of the procurement/ tendering procedures and actual tenders;

(h) assessment OF the completeness and effectiveness of the outsourcing policy;

(i) assessment of the completeness and adequacy of the credit institution's business continuity and the information technology disaster recovery plans;

(j) assessment of the completeness and adequacy of the credit institution's information security policy, including information technology security;

(k) assessment of the process for assessing the credit institution's Internal Capital Adequacy Assessment Process (ICAAP) in relation to its risk profile, the parameters upon which the credit institution has based its capital adequacy calculations and the review of the process for stress testing the credit institution's capital levels, taking into account the frequency of such exercises, their purpose, the reasonableness of scenarios, the underlying assumptions employed and the reliability of the processes used;

(l) assessment of the extent to which the approval procedures for new product developments are applied in accordance with the new products approval policy and whether these procedures are adequate and effective;

(m) assessment of the appropriateness of the remuneration policy in relation to the predetermined goals set by the legal and regulatory framework, and the possible consequences of the policy in the assumption and management of risks;

(n) assessment of the adequateness and enforceability of the claw back arrangements as well as the structure of the bonuses regarding the deferred payment element requirements and its linkage with future performance within a reasonable time horizon;

(o) assessment of the adequacy and effectiveness of the compliance function, risk management function and ICT and security function.

Audit plan.

79.- (1) The audit plan shall be risk-based and dynamic, aiming to ensure all entities and all activities of the credit institution are audited at least once within an appropriate period of time. The audit plan shall be a means of assessing the adequacy and effectiveness of the internal control framework.

(2) The audit plan shall ensure that as a minimum:

(a) credit review inspections of an appropriate scale are carried out on an annual basis as a means for assessing:

(i) the adequacy and effectiveness of, and adherence to, the credit granting procedures and policy, including the procedures for the assessment of credit applications and approval of credit facilities, as well as on the management and monitoring mechanism of collaterals and securing compliance with the credit covenants, in accordance with the Directive of the Central Bank on Credit Granting and Review Processes;

(ii) the correct application of the internal credit rating system developed by the credit institutions in accordance with the guidelines of the Central Bank in relation to the management of credit risk;

(iii) the appropriateness, adequacy and correct implementation of the provisioning policy as well as on the adequacy of the provisions and the completeness of the methodology and procedure for the calculation of the loan impairments, including the selection criteria of loans for impairment testing;

(iv) the completeness of the methodology and procedure for the calculation of the impairment of other assets as well as of the adequacy of the relevant provisions and impairment write-offs;

(v) the adequacy of the monitoring procedures and handling of non-performing and problematic loans;

(vi) the adequacy and effectiveness of relevant internal controls;

(b) the adequacy of, and adherence to, the procedures for granting credit facilities to members of the management body and connected persons, major shareholders and connected persons is assessed on annual basis;

(c) special inspections of an appropriate scale are carried out on an annual basis as a means for assessing the adequacy and effectiveness of information systems and information security;

(d) the effectiveness and adequacy of the policy, procedures and controls for the prevention of money laundering and terrorist financing, and the level of compliance with the provisions of the Prevention and Suppression of Money Laundering Activities Law of 2007 and its subsequent amendments and the Prevention of Money Laundering and Terrorist Financing Directive of 2013 is assessed on an annual basis;

(e) the adequacy and completeness of the outsourcing policy is assessed at least every three years and corrective measures are followed-up on an annual basis; in addition, the internal audit function shall carry out annual assessments of outsourced services or activities of an appropriate scale as a means for to assessing the adherence to the outsourcing policy giving priority to the outsourcing of critical or important services or activities to third parties;

(f) the application of the remuneration policy by the senior management and its compliance with the relevant policies and procedures adopted by the management body is assessed at least on an annual basis.

Reporting requirements of the internal audit function.

80.- (1) The head of the internal audit function shall report to the management body through the audit committee, at least on a quarterly basis, at least on a quarterly basis emanating from the audits carried out since the last report to the management body as well as recommendations for addressing any weaknesses identified; when weaknesses of significance are identified, the head of the internal audit has the responsibility to communicate them as soon as practically possible to the management body.

(2) The head of the internal audit function shall submit an annual report to the management body, within two months from the end of each year, through the audit committee, which will also be copied to the chief executive, with the following minimum information:

(a) the audit plan approved by the management body for the year under review and the rationale for any deviations in its implementation υ;

(b) summary, coupled with comprehensive comments, of the major findings and weaknesses identified from the routine inspections and special audits carried out during the year under review for each audited area;

(c) an up-to-date summary of the progress achieved in the implementation and the effectiveness of the corrective actions taken in addressing any weaknesses and findings identified in the various inspection reports of the internal and external auditors as well as those of the supervisory authorities;

(d) verification on a sample basis of the accuracy of the returns submitted to the competent authority;

(e) the audit and action plan for the following year.

Cooperation between the internal audit function and the competent authority.

81.- The head of the internal audit function's cooperation with the competent authority shall cover the following topics, based on the results of the assessments carried out:

(a) the adequacy and effectiveness of the credit institution's processes for objective setting and strategic decision making;

(b) the quality and substance of management and governance structure and processes;

(c) the credit institution's capital and liquidity positions and its processes and methods for identifying, monitoring, controlling, and reporting on material risks including the risks referred to in paragraphs 45 to 54;

(d) the credit institution's business model including risks in the credit institution's business activities, processes and functions and the adequacy of the control and oversight of these risks such as:

(i) implementation and application of risk management procedures and risk assessment methodologies as applied to material risks including the risks referred to in paragraphs 63 to 71;

(ii) appropriateness and adequacy of the provisioning policy as well as on the adequacy of the provisions;

(iii) completeness of the impairment / write-off methodology;

(iv) adequate management significant transactions;

(v) handling of non-performing and problematic loans;

(vi) management of fraud / fraud risk management;

(vii) management of tasks outsourced to third parties;

(e) ethics issues such as:

(i) management of conflicts of interest;

(ii) compliance with the rules in the provision of services to customers;

(iii) procedures and controls to combat money laundering;

(f) issues related to the internal control function and the adequacy and effectiveness of the other functions of the internal audit system.

External assessment of the adequacy of the internal control framework.

82.- (1) Credit institutions shall assign at least once every three years the assessment of the adequacy and effectiveness of their internal control framework to an external auditor other than the credit institution's statutory external auditor, who possess the necessary expertise in carrying out the required assessment in accordance with the provisions of Annex II.

(2) The assessment referred to in sub-paragraph (1) of this paragraph shall be prepared on a consolidated basis as well as on an individual basis. Prior to the commencement of the assessment tasks, the audit committee of the credit institution must determine the units and subsidiaries that will be included in the scope of the assessment. This shall be based on the principle of proportionality, as well as on other quality criteria. The scope of the assessment must be submitted in advance to the competent authority.

(3) Credit institutions shall rotate external auditors referred to in sub-paragraph (1) of this paragraph, after two consecutive assessments.

PART 10 – BUSINESS CONTINUITY MANAGEMENT

Business continuity management.

83.- (1) Credit institutions shall establish a sound business continuity management plan to ensure their ability to operate on an ongoing basis and to limit losses in the event of severe business disruption.

(2) Credit institutions may establish a specific independent business continuity function, for instance as part of the risk management function.

(3) A credit institution's business relies on several critical resources, such as IT systems, communication systems, key staff and buildings. The purpose of business continuity management is to reduce the operational, financial, legal, reputational and other material consequences arising from a disaster or extended interruption to these resources and consequent disruption to the credit institution's ordinary business procedures. Other risk management measures might be intended to reduce the probability of such incidents or to transfer their financial impact to third parties (for instance through insurance against risks).

(4) In order to establish a sound business continuity management plan, the credit institution shall carefully analyse its exposure to severe business disruptions and assess (quantitatively and qualitatively) their potential impact, using internal and/or external data and scenario analysis. This

analysis shall cover all business lines and internal units, including the risk management function, and shall take into account their interdependency. The results of the analysis shall contribute to defining the credit institution's recovery priorities and objectives.

(5) On the basis of the abovementioned analysis, a credit institution shall put in place:

(a) contingency and business continuity plans to ensure that the credit institution reacts appropriately to emergencies and is able to maintain its most important business activities if there is disruption to its ordinary business procedures; and

(b) recovery plans for critical resources to enable the credit institution to return to ordinary business procedures in an appropriate timeframe. Any residual risk from potential business disruptions shall be consistent with the credit institution's risk appetite.

(6) Contingency, business continuity and recovery plans shall be documented and carefully implemented. The documentation shall be available within the business lines, internal units and RMF, and shall be stored on systems that are physically separated and readily accessible in case of contingency. Appropriate training shall be provided. Plans shall be regularly tested and updated. Any challenges or failures occurring in the tests shall be documented and analysed, with the plans reviewed accordingly.

PART 11 – TRANSPARENCY

Transparency.

84.- (1) Strategies, policies and procedures shall be communicated to all relevant staff throughout a credit institution. A credit institution's staff shall understand and adhere to policies and procedures pertaining to their duties and responsibilities.

(2) The management body shall inform and update the relevant staff about the credit institution's strategies and policies in a clear and consistent way, at least to the level needed to carry out their particular duties. This may be done through written guidelines, manuals or other means.

Publications.

85.- (1) Credit institutions which are parent undertakings, are required to publish annually a description of their legal structure and governance and the organisational structure of the group of credit institutions, in accordance with paragraph (c) of subsection (3A) of section 24 of the Law. the information shall include all entities within the group structure.

Provided that for the purposes of this paragraph «group» is defined according to article 4 paragraph 1 point 138) of Regulation (EU) 575/2013.

(2) The publication shall include at least:

(a) an overview of the internal organisation of the credit institutions and the group structure, and changes thereto, including the main reporting lines and responsibilities;

(b) any material changes since the previous publication and the date of the material change;

(c) new legal, governance or organisational structures;

(d) information on the structure, organisation and members of the management body, including the number of its members and the number of those qualified as independent, and specifying the gender and duration of the mandate of each member of the management body;

(e) the key responsibilities of the management body;

(f) a list of the committees of the management body in its supervisory function and their composition;

(g) an overview of the conflict-of-interest policy applicable to the credit institutions and to the management body;

(h) an overview of the internal control framework;

(i) an overview of the business continuity management framework; and

(j) when a credit institution is state owned, the general objectives of state ownership, including any specific obligations of the credit institution regarding the social policy of the state, how these obligations are financed as well as the policy and role of the state in the Internal Governance of the credit institution.

(3) In cases where a high level of accuracy could delay the communication of time-sensitive information, the credit institution shall make a decision on finding the right balance between timing and accuracy, taking into account the requirement to present a true and fair view of its situation and provide a satisfactory explanation for any delay, this explanation shall not be used to delay the submission of regularly required reports.

(4) Credit institutions shall explain on their website how they comply with the requirements of the harmonising provisions of Articles 88 to 95 of Directive 2013/36/EU:

(a) concerning Article 88, in sub-paragraph (1) of paragraph 6 and in points (a) to (d) of sub-paragraph (2) of paragraph 6, in sub-paragraph (10) of paragraph 7 and in paragraph 23 of this Directive as well as section 19B(2) of the Law;

(b) concerning Article 89, in section 24A of the Law;

(c) concerning Article 90, in section 24B of the Law;

(d) concerning Article 91, in points (e) and (f) of sub-paragraph (2) of paragraph 6 and sub-paragraphs (1) and (5) of paragraph 15, in point (d) of sub-paragraph (1) of paragraph 26 and in point (c) of sub-paragraph (5) of paragraph 83 of this Directive, in sub-paragraph (3) of paragraph 12 of the Assessment of the Suitability of Members of the Management Body and Persons holding Key Positions in Licensed Credit institutions Directives of 2020 and in sub-section (1) of section 26 of the Law;

(e) concerning Article 92, in sub-paragraph (2) of paragraph 30 of this Directive;

(f) concerning Article 93, in paragraph 32 of this Directive;

(g) concerning Article 94, in paragraph 31 of this Directive;

(h) concerning Article 95, in sub-paragraph (1) of paragraph 17, in sub-paragraph (5) of paragraph 18 and in sub-paragraphs (1) to (3) of paragraph 22 of this Directive.

PART 12 – REPORTING TO THE COMPETENT AUTHORITY

Reporting to the competent authority.

86.- (1) Credit institutions shall submit to the competent authority the final minutes of the meetings of the management body, of the audit committee and of the risk committee, as foreseen by paragraphs 12 and 19 of this Directive, within one (1) month from the date of the meeting. In case a meeting of the management body does not take place within one (1) month, the minutes shall be approved by written procedure by all members present at the meeting and shall be submitted to the competent authority within the specified time limit.

(2) Credit institutions shall submit the following reports and information to the competent authority, within three (3) months from the end of each year, accompanied by the respective evaluations of the competent committees of the management body and the relevant excerpts from the minutes of the meetings of the management body:

(a) an annual report on the internal control framework to be prepared by the head of the internal audit function;

(b) an annual report on risk management, to be prepared by the head of the risk management function;

(c) an annual report on regulatory compliance, to be prepared by the head of the compliance function;

(d) an assessment report of the performance of the management body in its entirety, of the committees and of the individual members, to be prepared by the management body in accordance with the provisions of paragraph 16 of this Directive including the assessment of the chair of the management body referred to in paragraph 11 of this Directive;

(3) Credit institutions shall submit to the competent authority the annual report on information security, referred to in paragraph 75. The annual report shall be submitted within two (2) months of the end of the reporting period.

31(I) of 2018
32(I) of 2019.

This report shall take into account and cover the requirements of paragraph (2) of section 95 of the Provision and Use of Payment Services and Access to Payment Systems Law of 2018.

(4) Credit institutions shall submit to the competent authority the annual report of the Outsourcing Officer to third parties, in accordance with the provisions of sub-paragraph (6) of paragraph 38 of this Directive.

(5) Credit shall credit institutions submit to the competent authority on an annual basis until June 30 of each year:

EBA/GL/2014/08
16.07.2014

(a) for the purposes of section 26D of the Law, the standards set out in Annexes 1-3 to the EBA Guidelines on the Comparative Salary Assessment of 2014, in accordance with the requirements specified in Titles III and IV of the said EBA Guidelines;

EBA/GL/2014/07
16.07.2014

(b) for the purposes of section 26C (2) of the Law, the standards set out in Schedule 1 of the EBA Guidelines on the collection of data on highly paid persons of 2014, in accordance with the requirements specified in Titles II and III of the said guidelines.

(6) Credit institutions shall submit to the competent authority, within a reasonable time and in consultation with the competent authority, the assessment reports on the adequacy and effectiveness of the internal control framework on an individual and consolidated basis, which are prepared by the external auditors in accordance with the provisions of paragraph 82 of this Directive.

(7) Credit institutions shall submit to the competent authority, within a reasonable time and in consultation with the competent authority, the assessment reports on the composition, efficiency and effectiveness of the management body and its committees, which shall be prepared by an external consultant in accordance with the provisions of sub-paragraph (2) of paragraph 16 of this Directive.

PART 13 – MISCELLANEOUS PROVISIONS

Repeal.

87. – The Governance and Management Arrangements Directive of 2014 issued by the Central Bank to credit institutions, is hereby repealed.

Entry into force.

88.- The provisions of this Directive shall enter into force on the day of its publication in the Official Gazette of the Republic.

Annex I

ANNEX I – ASPECTS TO TAKE INTO ACCOUNT WHEN DEVELOPING AN INTERNAL GOVERNANCE POLICY

In accordance with Part 6, credit institutions shall consider the following aspects when documenting internal governance policies and arrangements:

1. Shareholder structure

2. Group structure, if applicable (legal and functional structure)

3. Composition and functioning of the management body

(a) selection criteria, including the way in which diversity is taken into account

(b) number, length of mandate, rotation, age

(c) independent members of the management body

(d) executive members of the management body

(e) non-executive members of the management body

(f) internal division of tasks, if applicable

4. Governance structure and organisation chart (with impact on the group, as the case may be)

(a) specialised committees

(i) composition

(ii) functioning

(b) executive committee, if any

(i) composition

(ii) functioning

5. Key function holders

(a) head of the risk management function

(b) head of the compliance function

(c) head of the internal audit function

(d) head of the ICT and security risk management function

(e) chief financial officer

(f) other key function holders

6. Internal control framework

(a) description of each function, including its organisation, resources, stature and authority

(b) description of the risk management framework, including the risk strategy

7. Organisational structure (with impact on the group, if applicable)

(a) operational structure, business lines, and allocation of competences and responsibilities

(b) outsourcing arrangements

(c) range of products and services

(d) geographical scope of business activities

(e) free provision of services

(f) branches

(g) subsidiaries, joint ventures, etc.

(h) use of offshore centres

8. Code of conduct and behaviour (with impact on the group, if applicable))

(a) strategic objectives and company values

(b) internal codes and regulations, prevention policy

(c) conflict of interest policy

(d) whistleblowing

9. Status of the internal governance policy, with date

(a) development

(b) last amendment

(c) last assessment

(d) approval by the management body.

Annex II

CONTENTS OF THE REPORT ON THE ASSESSMENT OF THE ADEQUACY OF THE INTERNAL CONTROL FRAMEWORK TO BE PREPARED BY EXTERNAL AUDITORS

PART I – INTRODUCTION

1. (1) The assessment shall be carried out in accordance with best international practices in order to ensure that the internal control system meets the standards required in this Directive.

(2) The assessment on the adequacy of the internal control framework shall cover the review of:

(a) the control environment;

(b) the risk assessment process;

(c) the security mechanisms and controls;

(d) the communication channels and information technology systems;

(e) the role, duties and responsibilities of the management body and the internal control functions; and

(f) the functioning, staffing of the credit institution's key departments / divisions / units, their terms of reference, procedures and information technology used.

2. Upon completion of the assessment, the external auditors shall issue a report expressing their opinions on the adequacy of the Internal Control System and prepare an analytical report with their observations / weaknesses identified and their recommendations for corrective actions. The aforesaid report shall be reviewed by the credit institution's audit committee.

PART II - MINIMUM ASPECTS OF ASSESSMENT

3. The report shall cover, as a minimum, assessment / examination of the following:

(a) Organisational structure

(i) The organisational structure (organisational chart and reporting lines, composition, terms of reference and functioning of the management body and its committees);

(ii) An assessment whether the general framework for corporate governance complies with the provisions of this Directive and ensures prompt and precise communication of all material issues relating to the credit institution;

(iii) The adequacy of the systems used for the production of information in accordance with the related legal / regulatory framework;

(iv) The role of the management body in relation to ensuring the adequacy of the internal control system;

(v) Conflict of interests, four eyes principle and segregation of duties; and

(vi) The procedure for the preparation of the annual budget in line with the credit institution's strategy and procedures to be followed in cases of deviations from the said strategy.

(b) Accounting system

During the examination of the accounting system, the adequacy of the internal control system in relation to the preparation of reliable financial statements shall be assessed. The assessment shall cover the ability of the management information system which facilitates the timely and reliable flow of the required information to every officer or administrative unit, in order to enable them to discharge their duties.

(c) Information technology systems

(i) Organisation and governance of information technology systems;

(ii) development and commissioning of systems;

(iii) systems operation and support;

(iv) physical and logical security;

(v) electronic and mobile banking; and

(vi) Business continuity and disaster recovery plans.

(d) Audit committee and internal audit function

(i) Assessment of the audit committee as to its membership, its duties, involvement in the audit procedure, the annual report on the internal control system prepared by the head of the internal audit function and the briefing of the management body.

(ii) In relation to the head of the internal audit function, his independence, his position on the organisational chart and his connection to the management body and to the audit committee shall be examined;

(iii) practices and internal audit methodology which shall be compared with best practices;

(iv) internal audit system (for the storage of audit programs, plans, findings, recommendations and for the generation of management reports) and computer assisted audit techniques, if any, used by the credit institution;

(v) on a sample basis, the adequacy of audit reports for the credit institution and its subsidiaries prepared by the internal audit function;

(vi) the monitoring procedure for the compliance of audited units with the recommendations of the head of the internal audit function; and

(vii) external quality assessment review of the internal audit function.

(e) Risks committee and risk management function

(i) composition and role of the risk committee;

(ii) e framework for the management of risks and, more specifically, whether there are adequate mechanisms for identification, monitoring and management of all types of risks incurred by the credit institution;

(iii) measures to be taken when emergency liquidity problems arise;

(iv) independence, roles and responsibilities and the work performed by the risk management function and its head;

(v) adequacy and effectiveness of risk management policies and procedures (including loan loss provisioning methodology);

(vi) the possibility of different risk management procedures in other countries in which the credit institution has presence;

(vii) the procedure for the evaluation of the risks involved in the design of new products / launch of a new service;

(viii) the objectivity of the procedures for the assessment of credit applications and approval of credit facilities, the tools used for the internal credit rating of facilities, the management and monitoring mechanism of collaterals and compliance with the credit covenants, the measures taken for dealing with non-performing loans and the capability of monitoring risks in the entire loan portfolio of the credit institution; an

(ix) adequacy and adherence to the procedures for granting credit facilities to members of the management body and connected persons as well as to other persons who maintain a special relationship with the credit institution and for securing their non-preferential treatment.

(f) Compliance function

(i) An assessment of the compliance function as to its independence, roles and responsibilities, its access to all sources of information, the prompt and reliable communication of its findings and the effective adoption of changes in the regulatory framework;

(ii) adequacy and effectiveness of policies and procedures as well as the management body’s and senior management’s responsibilities for the management of compliance risk; and

(iii) adequacy of the procedures in place for the prevention and suppression of money laundering and terrorist financing and the procedure for classifying transactions and counterparties into the various risk categories.

(g) ICT and security risk management function

(i) Assessment of the ICT and security risk management function as to its independence, roles and responsibilities, its access to all sources of information, the prompt and reliable communication of its findings and the effective adoption of changes in the information security framework;

(ii) adequacy and effectiveness of the information security framework, as well as the management body's and senior management's responsibilities for overseeing information risk;

(iii) adequacy of the policies and procedures in place for effective management of ICT and security risks, as well as their effective handling;

(iv) existence of adequate monitoring and reviewing processes for the purpose of σ continuously improving information security in the credit institution.

5. Where the credit institution has a parent financing holding company and/or subsidiaries, the assessment of the internal control system of the said entities shall be carried out in the same way.